more security. usd

HOTELVERBAND IHA DEUTSCHLAND

ConCardis

Kreditkartensicherheit für Hotels

Wie PCI DSS die Geschäftstätigkeit nachhaltig sichert

ConCardis GmbH
Helfmann-Park 7
65760 Eschborn

www.concardis.com

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 zu einer Rufschädigung, die kaum noch zu beheben ist. Das Vertrauen der Kunden schwindet und die Geschäftstätigkeit trägt einen nachhaltigen Schaden davon.

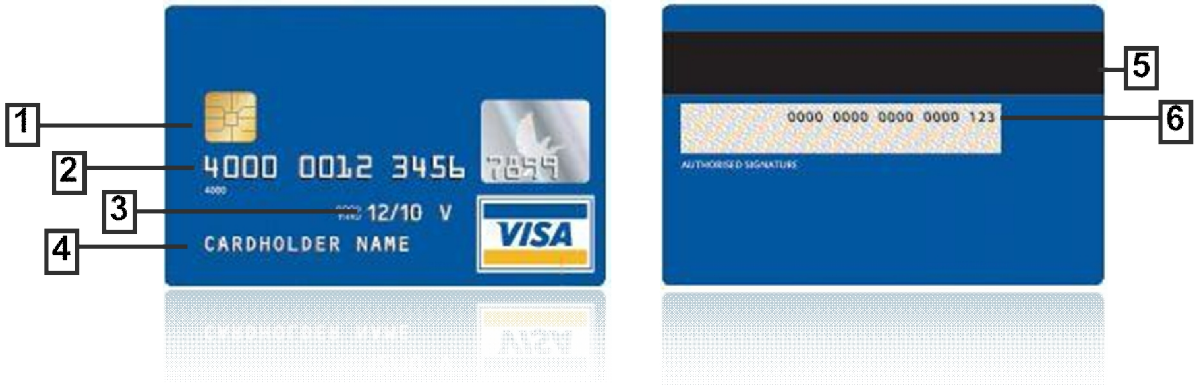
Um dem entgegenzuwirken, haben sich die großen Kreditkartengesellschaften zusammengeschlossen und das Payment Card Industry Security Standards Council (PCI SSC) gegründet. Durch die Vereinheitlichung der Sicherheitsleitlinien der einzelnen Gesellschaften entstand der PCI Data Security Standard (PCI DSS). 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.

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 fünf 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 Ihrer Händlerbank oder als Download von den Webseiten des PCI SSC unter:
https://www.pcisecuritystandards.org/security_standards/documents.php.

Beispiel: In meinem Hotel werden zur Zahlung mit Kreditkarte zwei ISDN-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	13 Fragen	▪ Alle Kreditkartenfunktionen ausgelagert ▪ Keine physische Präsenz von Kreditkarten (d.h. nur E-Commerce oder Versandhandel)
B	29 Fragen	▪ Es werden ausschließlich Terminals mit Wählverbindung (ISDN oder analog) zur Kreditkartenzahlung eingesetzt ▪ Keine elektronische Speicherung von Kreditkartendaten (auch nicht vom Terminal!)
C-VT	51 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	80 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	288 Fragen	▪ Alle, die nicht in den Beschreibungen für SAQ A bis C oben enthalten ▪ 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 Kategorien A bis C 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 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 C 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 erfolgen. 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.

Wird eine Fernwartung ohne Techniken vorgenommen, die diesen Vorgang absichern, ist SAQ D anzuwenden!

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 ISDN-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 http://de.pcisecuritystandards.org/minisite/en/saq-v2.0-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

Überprüfung der Zugriffsrechte (Wer hat Zugriff/Zugang?)

Gegebenenfalls Anpassungen vornehmen

3.3. Umgang mit E-Mails

Potentielles Risiko

Häufig versenden Kunden eine E-Mail an das Hotel, die ihre Kreditkartendaten enthalten, 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.

Aufgabe 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 Aktenver-

nichtung 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 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. Darüber hinaus können Sie auf den Webseiten des PCI Councils herausfinden, ob das von Ihnen eingesetzte Kartenterminal eine gültige Zertifizierung nach PCI PTS (PIN Transaction Security) aufweist. Ist dies der Fall, dann können Sie davon ausgehen, dass das Gerät mit den Anforderungen des PCI DSS vereinbar ist. Die Liste zertifizierter Kartenterminals finden Sie unter folgendem Link:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Aufgaben aus diesem Abschnitt
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 den Begriff der Endbenutzer-Technologien fallen generell unverschlüsselte E-Mails, Instant Messenger und Chat-Programme, wie beispielsweise ICQ oder Skype. 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 und mit Unterschrift auf einem Formular bestätigt werden, dass die Richtlinie gelesen und verstanden wurde.

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

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, hilft dabei, den Überblick zu behalten.

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 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 Liste mit Zugriffs- und Zugangsberechtigungen

Anfertigen Liste externer Dienstleister

Überprüfung des Status zur PCI DSS-Konformität der Dienstleister

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

Der Kreditkartenfluss im Hotel ist bekannt?	☐
Kreditkarten werden nur durch ein Terminal mit Wählverbindung (ISDN oder analog) 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 erden?	☐
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?	☐
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?	☐

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 C)

- Kreditkartendaten werden von Terminals oder Zahlungsanwendungen mit Internetverbindung verarbeitet.
- Keine elektronische Speicherung von Kreditkarteninformationen.

4.1. Anwendungsbereich

Die bis zu diesem Punkt behandelten Maßnahmen entsprechen denen eines Geschäftsmodells, in dem Kreditkartendaten ausschließlich mit Terminals mit Wählverbindung und Papierbelegen verarbeitet werden, ohne elektronische Speicherung dieser Informationen. Werden in Ihrem Hotel die Kreditkarten über Terminals oder Zahlungsanwendungen verarbeitet, die mit dem Internet verbunden sind, so ist der SAQ der Kategorie C anzuwenden. Voraussetzung ist, dass keine Kreditkarteninformationen elektronisch gespeichert werden und die Kreditkartenterminals und/oder Zahlungsanwendungssysteme ausschließlich mit dem Internet und keinem anderen System des Hotels verbunden sind. Die Nutzung des Internets zur Übertragung von Kreditkartendaten bietet Kriminellen eine zusätzliche Angriffsfläche, die nicht zu unterschätzen ist. Dies bedeutet, dass zu den Maßnahmen des vorangehenden Abschnitts einige Maßnahmen hinzukommen, um dem erhöhten Gefahrenpotential angemessen zu begegnen.

Die nachfolgend beschriebenen Maßnahmen sind größtenteils sehr technischer Natur. Sie umfassen weite Teile Ihrer IT-Infrastruktur, u.a. Rechner, den Internetzugang, die Vernetzung der verschiedenen Arbeitsplatzrechner untereinander. Falls Sie diese nicht selbst betreiben, so sollten Sie Ihren IT-Dienstleister fragen, ob die beschriebenen Maßnahmen umgesetzt sind bzw. diesen mit der Umsetzung beauftragen.

4.2. Sicherung des Netzwerks

Potentielles Risiko

Häufig gewähren unzureichend gesicherte Netzwerke einem Hacker leichten Zugriff auf die einzelnen Rechner, welche darin betrieben werden. Sind in einem Netzwerk keine Kontrollinstanzen vorhanden, die den Datenverkehr regulieren, so kann es zu unerwünschter Kommunikation und damit zu ungewünschten Zugriffen auf Rechner kommen. Insbesondere im Netzwerk befindliche Schwachstellen werden von Kriminellen gezielt ausgenutzt. Aber auch das geschickte Platzieren eines WLAN Access Points kann dafür sorgen, dass Kreditkartendaten unbemerkt in die Hände eines Hackers gelangen.

Maßnahmen

Eine Firewall reguliert den erlaubten ein- und ausgehenden Datenverkehr auf der Basis von festlegbaren Regeln. Auf diesem Wege können Zugriffe von außen auf Rechner innerhalb Ihres Hotels beschränkt werden. Dies gilt auch für die Kommunikation der Systeme innerhalb des Hotels. Die Kreditkartenterminals und/oder Zahlungsanwendungssysteme dürfen ausschließlich mit dem Internet verbunden sein. Eine Kommunikation zu anderen Systemen des Hotels, wie beispielsweise dem Warenwirtschaftssystem, darf nicht möglich sein. Durch den Einsatz und die geeignete Konfiguration von Firewalls kann die für die Anwendbarkeit des SAQ C geforderte Isolierung der entsprechenden Systeme erreicht werden. Um hinsichtlich der in Ihrem Hotel zu verarbeitenden Kreditkartendaten effizienten Schutz zu liefern, sollte eine Firewall die im Teil „Aufgaben aus diesem Abschnitt“ genannten Funktionen mitbringen.

Um unautorisierten Zugriffen vorzubeugen, ist es nötig das Netzwerk zu überwachen. Unbemerkt im Netzwerk platzierte WLAN Access Points können beispielsweise über eine physische Kontrolle, eine Begutachtung aller Netzwerkzugangsmöglichkeiten oder aber über Sicherheitsscans mit Software-Werkzeugen entdeckt werden. Da sie ein besonderes Risiko darstellen, müssen WLANs grundsätzlich von Systemen, die mit Kreditkartendaten arbeiten, durch eine Firewall getrennt werden.

Die an dieser Stelle und in den folgenden Abschnitten beschriebenen Maßnahmen zum Schutz von WLANs betreffen nur diejenigen, über die Kreditkartendaten übertragen werden. Empfohlen wird jedoch, diese Maßnahmen auch für andere WLANs umzusetzen. Andere Schwachstellen im Netzwerk werden durch sogenannte Schwachstellenscans aufgedeckt und sollten im Anschluss behoben werden. Dabei wird zwischen internen und externen Scans unterschieden. Erstere gehen dabei von dem Szenario eines Kriminellen aus, der sich schon im internen Netzwerk befindet. Letztere von einem Hacker, der über das Internet versucht, Zugang zum Netzwerk zu erlangen. Der PCI-Sicherheitsstandard fordert für die Durchführung der externen Schwachstellenscans, dass diese von einem vom PCI Council akkreditierten Scan-Anbieter, einem so genannten „Approved Scanning Vendor“ (ASV), vorgenommen werden. Interne Scans können auch von Ihrem IT-Dienstleister durchgeführt werden.

Die folgenden Punkte sollten Sie mit Ihrem IT-Dienstleister besprechen und sich bestätigen lassen, dass diese wie gefordert in der Praxis umgesetzt sind.

Aufgaben aus diesem Abschnitt

Firewall- und Router-Konfiguration beschränken Kommunikation zwischen kreditkartenverarbeitenden Systemen und dem Internet

Kreditkartenterminals und/oder Zahlungsanwendungen sind ausschließlich mit dem Internet verbunden

WLAN ist durch eine Firewall von kreditkartenverarbeitenden Systemen getrennt

Diese kontrolliert jeglichen Datenverkehr zwischen WLAN und kreditkartenverarbeitenden Systemen

Ein- und ausgehender Datenverkehr der Systeme mit Kreditkartendaten ist auf das notwendige Minimum beschränkt

Jeder andere ein- und ausgehender Datenverkehr wird geblockt („Deny All“)

Direkte Kommunikation zwischen kreditkartenverarbeitenden Systemen und Internet nicht möglich (alle Verbindungen müssen über die Firewall laufen)

Jeder von kreditkartenverarbeitenden Systemen ausgehende Datenverkehr ist explizit freigegeben worden

Die Firewall unterstützt „Stateful Inspection“

Es wird vierteljährlich nach unautorisierten WLAN-Zugriffspunkten gesucht

Vierteljährlich werden interne Schwachstellenscans von dafür qualifiziertem Personal durchgeführt

Gefundene Schwachstellen werden behoben und zur Kontrolle ein wiederholter Scan durchgeführt

Vierteljährlich werden externe Schwachstellenscans von einem ASV durchgeführt

Interne und externe Schwachstellenscans werden nach jeder bedeutsamen Änderung am Netzwerk durchgeführt (beispielsweise bei Inbetriebnahme zusätzlicher Systeme, Änderung der Firewall-Regelsätze oder Änderungen am Aufbau des Netzwerks)

Externe Scans werden wiederholt, bis keine Schwachstellen mehr mit einer CVSS-Klassifizierung (CVSS Base Score) größer als 4.0 gefunden werden

4.3. Sicherung der Systeme

Potentielles Risiko

Die allgemeine Bedrohung durch Viren, Würmer und Trojaner ist eine ständig gegenwärtige Gefahr für die im Betrieb eingesetzten Rechner. Diese sogenannte Schadsoftware kann die Nutzbarkeit der eigenen Rechner erheblich beeinträchtigen oder sogar unmöglich machen. Insbesondere kann durch sie der Zugriff auf Rechner kontrolliert und dadurch können sensible Informationen, wie Kreditkartendaten, gestohlen werden.

Maßnahmen

Antivirenprogramme und Virenschutzsoftware sollen Schutz vor Schadsoftware bieten, die gezielt versucht, bekannte Schwachstellen und Verwundbarkeit auszunutzen. Da solche Virenschutzsoftware nur gegen solche Schadsoftware vorgehen kann, die sie „kennt“, ist es absolut notwendig die eingesetzten Antivirenprogramme immer auf aktuellem Stand zu halten.

Schadsoftware versucht in den meisten Fällen, Sicherheitslücken von auf dem Rechner installierter Software auszunutzen. Werden solche Sicherheitslücken bekannt, beginnt der Hersteller in der Regel damit, die Sicherheitslücke zu beheben. Dies geschieht normalerweise, indem er einen Patch herausgibt. Dabei handelt es sich um ein „Stück Software“, welches nachinstalliert wird, um die Sicherheitslücke zu schließen. Daher ist es neben der Aktualisierung von Antivirenprogrammen ebenso wichtig, kritische Sicherheitspatches der Hersteller für das Betriebssystem (Windows Updates) und die verwendeten Applikationen (z.B. Acrobat Reader) innerhalb eines Monats nach deren Erscheinen zu installieren.

In diesem Zusammenhang sei darauf hingewiesen, dass Schadsoftware nicht nur über die Internetverbindung auf die Rechner Ihrer Mitarbeiter gelangen kann. Mobile Datenträger, wie beispielsweise USB-Sticks oder tragbare Festplatten, stellen, gerade aufgrund ihrer Mobilität und dadurch vielseitigen Einsetzbarkeit, ein nicht zu unterschätzendes Risiko dar. Wenn ein Gebrauch der USB-Schnittstellen an den Arbeitsplatzrechnern der Mitarbeiter zur alltäglichen Geschäftstätigkeit nicht nötig ist, so ist deren Deaktivierung zu empfehlen.

Bitte überprüfen Sie, gegebenenfalls mit Ihrem IT-Dienstleister, ob die folgenden Punkte auf Ihren Systemen umgesetzt sind.

Aufgaben aus diesem Abschnitt

Antivirenprogramme/Virenschutzsoftware auf allen Rechnern installiert

Diese sind aktiv, up to date und protokollieren auffällige Vorkommnisse

Bieten Schutz vor jeglichem Typ von bekannter Schadsoftware (beispielsweise Virus, Trojaner, Würmer, Spyware, Adware, Rootkits)

Automatische Updates der Viren-Signaturen und regelmäßige komplette Viren-Scans sind voreingestellt (falls vorhanden, auch bei der Master-Installation)

Aktuelle Sicherheits-Patches der Hersteller werden mindestens monatlich installiert

4.4. Voreingestellte Herstellerstandards

Potentielles Risiko

Neu angeschaffte Software und Geräte bringen bei ihrer Auslieferung meist gewisse Voreinstellungen mit, die vom Hersteller standardmäßig vorgenommen werden. Dabei handelt es sich um einen ganz normalen Vorgang, der eine leichte Inbetriebnahme ermöglichen soll. Allerdings sind diese Voreinstellungen häufig recht einfach gehalten, so dass sie nur unzureichend Sicherheit bieten. Insbesondere wenn es sich dabei um voreingestellte Zugangsdaten wie Benutzername und Passwort handelt. Zudem sind weitere herstellerspezifische Voreinstellungen bekannt und als Information im Internet frei verfügbar. So wird ein Hacker beispielsweise versuchen herauszufinden, mit was für einer Software oder einem Gerät er es zu tun hat. Werden voreingestellte Passwörter nicht geändert, so kann diese Tatsache einen Hackerangriff erheblich begünstigen, da er anschließend die dafür bekannten Standard-Passwörter ausprobieren wird.

Maßnahmen

Zugangsdaten, wie Benutzername und Passwort, die vom Hersteller voreingestellt mit dem Produkt ausgeliefert werden, sind für Hacker oft leicht herauszufinden oder zu erraten. Daher sollten diese in jedem Fall geändert werden.

Wenn die von Ihnen eingesetzte Bezahlanwendung oder das Bezahlterminal über WLAN mit Ihrem Internetzugang verbunden ist, wird vom PCI-Sicherheitsstandard gefordert, dass folgende Änderungen der herstellerseitigen Voreinstellungen vorzunehmen sind. Bitte klären Sie, gegebenenfalls mit Ihrem IT-Dienstleister, ob für Ihre WLAN-Umgebung folgende Maßnahmen getroffen wurden.

Aufgaben aus diesem Abschnitt

Herstellerseitige Voreinstellungen werden bei Installation geändert (Änderung der Standard-Passwörter, Sperren bzw. Deaktivieren von nicht benötigten Accounts, die in der Gebrauchsanleitung des Herstellers genannte Sicherheitsmaßnahmen umsetzen)

Hinweis: Nach Möglichkeit auf die Nutzung von Kreditkartendatenübertragung mit WLAN verzichten.

WLAN, das Kreditkartendaten überträgt, erfüllt Folgendes:
Standardwerte der Verschlüsselung geändert

Schlüssel wird geändert, wenn ein Mitarbeiter, der ihn kennt, das Hotel verlässt

Standard-SNMP-Community-Zeichenfolgen sind geändert

Standard-Passwort für den WLAN-Zugriffspunkt ist geändert

Firmware ist auf dem aktuellen Stand

Soweit vorhanden, sind auch alle anderen sicherheitsrelevanten Voreinstellungen geändert

Auf den Systemen sind nur Dienste, Protokolle und Daemons aktiv,
die benötigt werden (alle anderen sind deaktiviert)

4.5. Sichere Übertragung von Kreditkartendaten

Potentielles Risiko

Werden zur elektronischen Übertragung von Kreditkartendaten öffentliche Netze verwendet, so ist es für Angreifer relativ einfach, diese Daten während der Übertragung abzufangen. Die Kriminellen bedienen sich dafür an einer Fülle von im Internet frei verfügbaren Programmen, um die Daten während ihres Transits abgreifen zu können. Sind diese Daten nicht verschlüsselt worden, so können sie von jedermann gelesen werden, auch von demjenigen, der sie unberechtigterweise abgegriffen hat. Insbesondere WLAN mit schwacher Verschlüsselung bieten Kriminellen eine relativ einfache Möglichkeit, die Daten unbemerkt abzufangen.

Maßnahmen

Um Daten vor solchem Missbrauch zu schützen, ist es wichtig diese für die Übertragung zu verschlüsseln. Sie können dann zwar immer noch von Hackern abgefangen werden, sind für diese aber aufgrund der Verschlüsselung nicht lesbar und damit unbrauchbar.

In diesem Zusammenhang spielen die Verschlüsselungs-Mechanismen eine zentrale Rolle. Diese müssen dem Versuch standhalten, von Hackern geknackt zu werden. Ist dies gewährleistet, so spricht man von einer „starken“ Verschlüsselung. Denn nur solch eine starke Verschlüsselung erfüllt ihren Zweck und bietet den nötigen Schutz für sensitive Daten. Daher sollten Sie mit Ihrem IT-Dienstleister klären, ob die im Folgenden genannten Schutzmechanismen umgesetzt sind.

Aufgaben aus diesem Abschnitt

Verwendung starker Verschlüsselung und Sicherheitsprotokolle

(beispielsweise SSL/TLS, SSH oder IPSEC)

Verwendung ausschließlich vertrauenswürdiger Zertifikate (z.B. von VeriSign, Thawte usw.)

Keine Verwendung von unsicheren Sicherheitsprotokollen (beispielsweise SSL v2.0 oder SSH v1.0)

Bei Verwendung von SSL ist HTTPS Bestandteil der Browser-URL

Arbeit mit Kreditkartendaten erst bei Anzeige von HTTPS in URL, bei Login-Seiten ebenfalls nur HTTPS-Login zulassen

Industrie-Standards für WLAN (starke Verschlüsselung für Übertragung und Authentisierung)

4.6. Arbeiten vom Heim-Arbeitsplatz

Potentielles Risiko

Aus technologischer Sicht stellt das Arbeiten vom heimischen Arbeitsplatz aus, dank Laptop und Internet, längst kein Problem mehr dar. Wenn dabei auf sensible Daten, wie beispielsweise Kreditkartendaten, die sich im Netzwerk des Hotels befinden, zugegriffen werden muss, muss sichergestellt werden, dass auch nur die Personen von außen diese Zugriffsmöglichkeit haben, die dazu auch befugt sind. Ansonsten könnte ein Krimineller vorgeben, er sei eine zugangsberechtigte Person, und so versuchen, auf Kreditkartendaten zuzugreifen und diese zu stehlen.

Maßnahmen

Neben der allgemeinen Sicherung der Kommunikationswege ist also bei Zugang von außen zum Netzwerk des Hotels sicherzustellen, dass dieser nur autorisierten Personen möglich ist. Der „Beweis“, dass sich hinter

der Person auch die verbirgt, die tatsächlich zugangsberechtigt ist, muss über eine sogenannte Zwei-Faktor-Authentisierung erfolgen.

Es werden im Allgemeinen drei Faktoren unterschieden, anhand derer die eigene Identität nachgewiesen werden kann:

1. Etwas, das man weiß: meist handelt es sich dabei um ein Passwort

2. Etwas, das man besitzt: kann beispielsweise eine Chipkarte sein

3. Etwas, das man ist: hierbei handelt es sich um biometrische Merkmale, beispielsweise ein Fingerabdruckscan

Einen einzigen Faktor zweimal zu verwenden, gilt nicht als Zwei-Faktor-Authentisierung. Werden beispielsweise zwei verschiedene Passwörter nacheinander abgefragt, entsteht kein Mehrgewinn an Sicherheit. Nur die Kombination von mindestens zwei verschiedenen Faktoren kann den Zweck von mehr Sicherheit erfüllen. Je mehr dieser Faktoren nun kombiniert werden, um jemanden zu identifizieren, desto schwieriger wird es für Kriminelle, diese Identität zu imitieren. Deshalb wird bei Zugriffen, die von außerhalb auf das Netzwerk des Hotels stattfinden sollen, der Nachweis der eigenen Identität anhand zweier der obigen drei Faktoren gefordert. Ihr IT-Dienstleister sollte Ihnen bei der Umsetzung die notwendige Hilfestellung bieten können.

Aufgaben aus diesem Abschnitt
Nachweis der Identität über mindestens zwei Faktoren ist zwingend erforderlich, um von außen auf das Hotelnetzwerk zugreifen zu können

4.7. Administrativer Zugriff und Fernwartung von Systemen

Potentielles Risiko

Wenn Systeme nicht über eine unmittelbar daran angeschlossene Konsole verwaltet werden, so kann ein schlecht gesicherter Fernzugriff dazu führen, dass ein Hacker sicherheitskritische Informationen in Erfahrung bringt. Im Falle schwacher oder gar fehlender Verschlüsselung könnte der Kriminelle beispielsweise Passwörter erbeuten, die ihm zu einem späteren Zeitpunkt Zugriff auf die Systeme, und damit auch auf Kreditkartendaten, ermöglichen.

Maßnahmen

Der Systemzugriff zu Verwaltungszwecken, der nicht direkt über einen an den Rechner angeschlossenen Bildschirm durchgeführt wird, muss über eine starke Verschlüsselung gesichert werden. Dabei stellt insbesondere der Anmeldevorgang ein Risiko dar, so dass darauf geachtet werden muss, dass Verschlüsselungsmechanismen schon greifen, bevor das Passwort abgefragt wird.

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. 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.

Aufgaben aus diesem Abschnitt
Nichtkonsolen-Verwaltungszugriffe werden mit starker Verschlüsselung (beispielsweise mit SSH, VPN oder SSL/TLS) geschützt

Aufruf starker Verschlüsselungsmethode vor Eingabe des Administrator-Passworts

Starke Verschlüsselung auch bei Administrator-Zugriff auf webbasierte Managementschnittstellen

Nutzung von unsicheren Remote-Anmeldeverfahren (beispielsweise Telnet oder rlogin) ist nicht möglich

Fernzugriffe meines IT-Dienstleisters oder eines Herstellers erfolgen ausschließlich über dafür eingerichtete Accounts

Diese Accounts sind nur aktiv, wenn sie benötigt werden

Während des Fernzugriffs sollten die Aktivitäten des Dienstleisters bzw. Herstellers beobachtet werden

4.8. Ergänzungen in den Sicherheits-Dokumenten

Die Erläuterungen im vorangegangenen Kapitel rund um eine Informationssicherheitsrichtlinie besitzen auch für den Anwendungsbereich des SAQ der Kategorie C ihre Gültigkeit. Aufgrund der Eigenschaften und Funktionsweise der eingesetzten Technologien sind aber einige Ergänzungen notwendig, um die durch sie entstandenen Risiken zu kommunizieren.

Informationssicherheitsrichtlinie

Die Informationssicherheitsrichtlinie sollte um die folgenden Inhalte ergänzt werden:

- Die Authentifizierung ist erforderlich, um nachzuweisen, dass die jeweilige Person tatsächlich zugriffsberechtigt ist. Ohne Mechanismen zum Identitätsnachweis könnten Kriminelle recht einfach auf Systeme zugreifen.
- „Akzeptable Netzwerkorte“ sollten festgelegt werden. Sie beschreiben, wo Rechner idealerweise stehen sollten, von denen auf Kreditkartendaten zugegriffen werden kann. Beispielsweise könnte festgelegt werden, dass Bildschirme derart aufgestellt sein müssen, dass Einblicke nicht möglich sind. Dies hilft dabei, den Überblick zu bewahren und eventuelle Sicherheitslücken zu identifizieren.
- Insbesondere die Verwendung von Technologien, die es erlauben, vom heimischen Arbeitsplatz aus auf das Hotelnetzwerk zuzugreifen, stellen ein Risikopotential dar. Deshalb sieht der PCI-Sicherheitsstandard vor, dass diese Technologien so konfiguriert sein müssen, diese Verbindungen nach einer gewissen Inaktivität (15 Minuten) automatisch zu unterbrechen und eine erneute Anmeldung mit Passwort zu fordern.
- Wird im Rahmen von Wartung und Support externen Dienstleistern oder einem Hersteller der Fernzugriff auf Systeme im Hotelnetzwerk gewährt, so sind für diesen Fall spezielle Maßnahmen zu treffen. Eine solche Zugriffsmöglichkeit stellt eine Art „Hintertür“ dar, die Zugang zu sensiblen Daten eröffnet. Daher ist es sehr wichtig, dass dieser Zugang nur dann aktiv ist, wenn er gerade benötigt wird, und ansonsten inaktiv ist.
- Die Notwendigkeit vierteljährlich nach unerlaubten WLAN Access Points zu suchen. Es sollte kurz beschrieben werden, wie dies umgesetzt wird. Alternativ kann eine Begehung aller Orte, die Zugangsmöglichkeiten zum Netzwerk des Hotels bieten, vorgenommen oder aber ein automatischer Scan durchge-

führt werden. Sollten Mitarbeiter im „Alltag“ einen unerlaubten WLAN-Zugriffspunkt entdecken, sollten diese angewiesen werden, diesen zu entfernen und den Vorfall der Hotelleitung zu melden.

Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten

Die Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten müssen insbesondere um diejenigen speziellen Punkte ergänzt werden, die den PCI-konformen Umgang mit den eingesetzten Technologien erläutern. Wenn Mitarbeitern erklärt wird, wie und warum sie etwas tun sollen, schafft dies die nötige Akzeptanz für die getroffenen Maßnahmen. Damit wird deren Einhaltung gefördert und Risiken durch Fehlverhalten eingegrenzt.

Abhängig vom Einsatz der jeweiligen Technologien sollten besonders die folgenden Punkte in den Arbeitsanweisungen berücksichtigt werden:

- Mitarbeiter, die dazu befugt sind, einem externen Dienstleister oder Hersteller im Rahmen von Wartung und Support Fernzugriff auf Rechner im Hotel zu gewähren, sollten mit dem Umgang dieser Zugangstechnologien vertraut sein. Es muss ihnen insbesondere klar sein, dass dieser Zugang sofort nach Beendigung der Support-Tätigkeit wieder zu deaktivieren ist und wie dies praktisch zu tun ist.

- Werden unerlaubte WLAN Access Points entdeckt, so sollten Mitarbeiter diese entfernen und den Vorfall der Hotelleitung melden.

Liste mit Zugriffs- und Zugangsberechtigungen

Die Liste mit Zugriffs- und Zugangsberechtigungen sollte nun auch erfassen, wer in welcher Weise auf Rechner zugreifen kann, die Kreditkartendaten verarbeiten. Es sollte in diesem Zusammenhang klar sein, wem entsprechende Passwörter bekannt sind und ob von Arbeitsplatzrechnern im Hotel oder vom heimischen Arbeitsplatz aus zugegriffen werden kann. Genauso muss geklärt sein, wer eventuell einem Dienstleister oder Hersteller den Zugang zum Hotelnetzwerk freigeben kann.

Liste externer Dienstleister

Auf der Liste externer Dienstleister sollten diejenigen mit einem speziellen Vermerk versehen werden, denen im Rahmen von Wartung und Support ein Fernzugriff auf Systeme im Hotelnetzwerk gewährt wird.

Aufgaben aus diesem Abschnitt

Ergänzen der Informationssicherheitsrichtlinie

Ergänzen der Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten

Ergänzen der Liste mit Zugriffs- und Zugangsberechtigungen

Ergänzen der Liste externer Dienstleister

4.9. Kreditkartendaten dauerhaft erfolgreich sichern

Für Geschäftsmodelle mit Kreditkartenverarbeitung über Terminals oder Zahlungsanwendungen mit Internetverbindung 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 nachzuweisen, können die Fragen des SAQ der Kategorie C mit „ja“ beantwortet werden, wenn die in diesem Handbuch beschriebenen Maßnahmen in Ihrem Hotel umgesetzt wurden. Für Technologien, die nicht eingesetzt werden, müssen selbstverständlich auch keine Maßnahmen umgesetzt werden. Im SAQ kann dann bei entsprechender Frage in der Spalte „Spezial“ als Antwort „Nicht anwendbar“ angegeben und im Anhang kurz erwähnt werden, warum diese Frage auf das eigene Hotel nicht zutreffend ist. Ist beispielsweise ein Fernzugriff auf Systeme von außerhalb des Hotels generell nicht erlaubt und nicht möglich, müssen Sie sich auch nicht mit den Maßnahmen befassen, die deren Sicherung zum Ziel haben.

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 DSS-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.

4.10. Anhang C: Checkliste SAQ – Kategorie C

Der Kreditkartenfluss im Hotel ist bekannt?	☐
Kreditkarten werden nur durch ein Terminal mit Wählverbindung (ISDN oder analog) 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 meinen 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?	☐
Beschränken die Firewall- und Router-Konfiguration die Kommunikation zwischen kreditkarten-verarbeitenden Systemen und dem Internet?	☐
Ist das WLAN durch eine Firewall von kreditkartenverarbeitenden Systemen getrennt?	☐
Kontrolliert die Firewall jeglichen Datenverkehr zwischen WLAN und kreditkartenverarbeitenden Systemen?	☐

Ist der ein- und ausgehende Datenverkehr der Systeme mit Kreditkartendaten auf das notwendige Minimum beschränkt?	☐
Wird jeder andere ein- und ausgehende Datenverkehr geblockt („Deny All“)?	☐
Ist eine direkte Kommunikation zwischen kreditkartenverarbeitenden Systemen und Internet nicht möglich (alle Verbindungen müssen über die Firewall laufen)?	☐
Sind Kreditkartenterminals und/oder Zahlungsanwendungen ausschließlich mit dem Internet und keinem anderen System im Hotel verbunden?	☐
Ist jeder von kreditkartenverarbeitenden Systemen ausgehende Datenverkehr explizit freigegeben worden?	☐
Wird von der Firewall Stateful Inspection unterstützt?	☐
Wird vierteljährlich nach unautorisierten WLAN Access Points gesucht?	☐
Werden vierteljährlich interne Schwachstellenscans von dafür qualifiziertem Personal durchgeführt?	☐
Werden gefundene Schwachstellen behoben und zur Kontrolle ein wiederholter Scan durchgeführt?	☐
Werden vierteljährlich externe Schwachstellenscans von einem ASV durchgeführt?	☐
Werden nach jeder bedeutsamen Änderung am Netzwerk interne und externe Schwachstellenscans durchgeführt (bspw. bei Inbetriebnahme zusätzlicher Systeme, Änderung der Firewall-Regelsätze oder Änderungen am Aufbau des Netzwerks)?	☐
Werden externe Scans wiederholt, bis keine Schwachstellen mehr mit einer CVSS-Klassifizierung größer als 4.0 gefunden werden?	☐
Sind auf allen Rechnern Antivirenprogramme/Virenschutzsoftware installiert?	☐
Sind diese aktiv, up to date und protokollieren auffällige Vorkommnisse?	☐
Bieten sie Schutz vor jeglichem Typ von bekannter Schadsoftware (bspw. Virus, Trojaner, Würmer, Spyware, Adware, Rootkits)?	☐
Sind automatische Updates der Viren-Signaturen und regelmäßige komplette Viren-Scans voreingestellt (falls vorhanden, auch bei der Master-Installation)?	☐
Werden aktuelle Sicherheits-Patches der Hersteller mindestens monatlich installiert?	☐
Werden sicherheitskritische Patches innerhalb eines Monats nach Erscheinen installiert?	☐
Werden herstellerseitige Voreinstellungen bei Installation geändert (Änderung der Standard-Passwörter, Sperren bzw. Deaktivieren von nicht benötigten Accounts u.a.)?	☐

Erfüllt das WLAN, das Kreditkartendaten überträgt, Folgendes?	
▪ Wurden Standardwerte der Verschlüsselung geändert?	☐
▪ Werden Schlüssel geändert, wenn ein Mitarbeiter, der sie kennt, das Hotel verlässt?	☐
▪ Wurden Standard-SNMP-Community-Zeichenfolgen geändert?	☐
▪ Wurde das Standard-Passwort für den WLAN-Zugriffspunkt geändert?	☐
▪ Ist die Firmware aktuell?	☐
▪ Soweit vorhanden, wurden alle anderen sicherheitsrelevanten Voreinstellungen geändert?	☐
Sind auf den Systemen nur Dienste, Protokolle und Daemons aktiv, die benötigt werden (alle anderen sind deaktiviert)?	☐
Werden zur Übertragung von Kreditkartendaten starke Verschlüsselung und Sicherheitsprotokolle (beispielsweise SSL/TLS, SSH oder IPSEC) verwendet?	☐
Werden ausschließlich vertrauenswürdige Zertifikate verwendet (z.B. von VeriSign, Thawte usw.)?	☐
Werden keine unsicheren Sicherheitsprotokolle (bspw. SSL v2.0 oder SSH v1.0) verwendet?	☐
Ist bei Verwendung von SSL der Ausdruck „HTTPS“ Bestandteil der Browser-URL?	☐
Ist die Arbeit mit Kreditkartendaten erst bei Anzeige von HTTPS in URL erlaubt?	☐
Werden Industrie-Standards für WLAN (starke Verschlüsselung für Übertragung und Authentisierung) verwendet?	☐
Ist Nachweis der Identität über mindestens zwei Faktoren zwingend erforderlich, um von außen auf das Hotelnetzwerk zugreifen zu können?	☐
Werden Nichtkonsolen-Verwaltungszugriffe mit starker Verschlüsselung (bspw. mit SSH, VPN oder SSL/TLS) geschützt?	☐
Wird vor Eingabe des Administrator-Passworts eine starke Verschlüsselungsmethode aufgerufen?	☐
Wird auch bei Administrator-Zugriff auf webbasierte Managementschnittstellen eine starke Verschlüsselung verwendet?	☐
Ist eine Nutzung von unsicheren Remote-Anmeldeverfahren (bspw. Telnet oder rlogin) nicht möglich?	☐
Sind Fernzugriffe meines IT-Dienstleisters oder eines Herstellers ausschließlich über dafür eingerichtete Accounts möglich?	☐

Sind diese Accounts nur dann aktiv, wenn sie auch benötigt werden?	☐
Werden die Aktivitäten des Dienstleisters bzw. Herstellers während des Zugriffs beobachtet?	☐
Existiert eine Informationssicherheitsrichtlinie mit den von SAQ B und C geforderten Inhalten?	☐
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?	☐
Wissen die Mitarbeiter, was zu tun ist, wenn sie nicht zulässige WLAN Access Points entdecken?	☐
Ist den Mitarbeitern, die mit Kreditkartendaten arbeiten, die Sensibilität dieser Daten bewusst?	☐
Besteht ein Vertragsverhältnis mit Dienstleistern, die mit Kreditkartendaten in Berührung kommen?	☐
Welchem Dienstleister oder Hersteller wird Fernzugriff auf das Hotelnetzwerk gewährt?	☐
Existiert eine Liste dieser Dienstleister?	☐
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?	☐