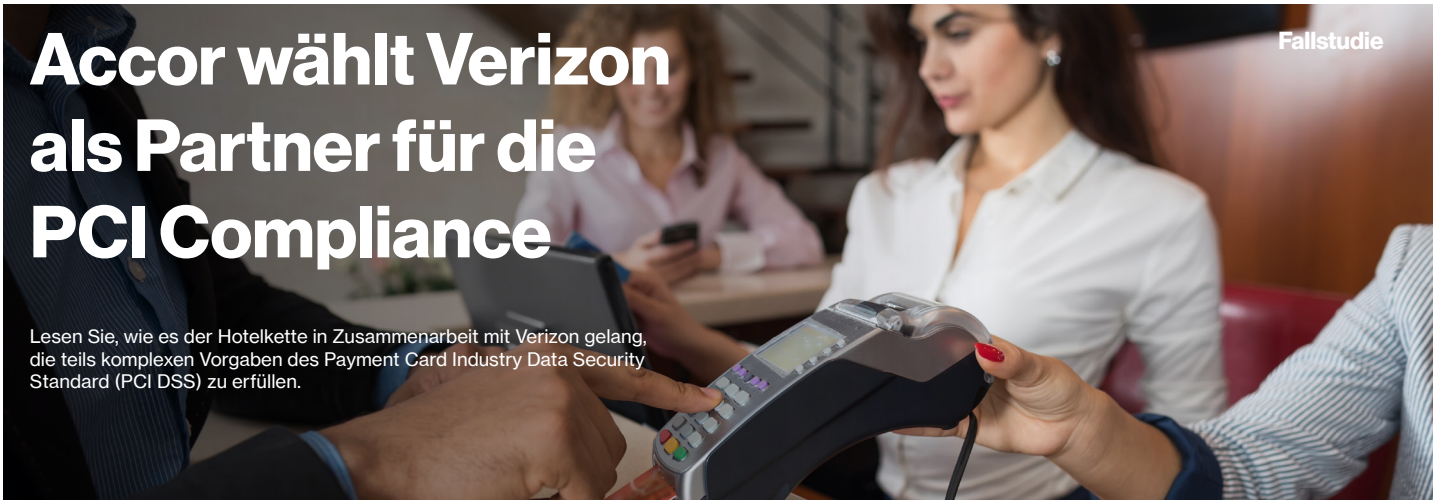


Fallstudie

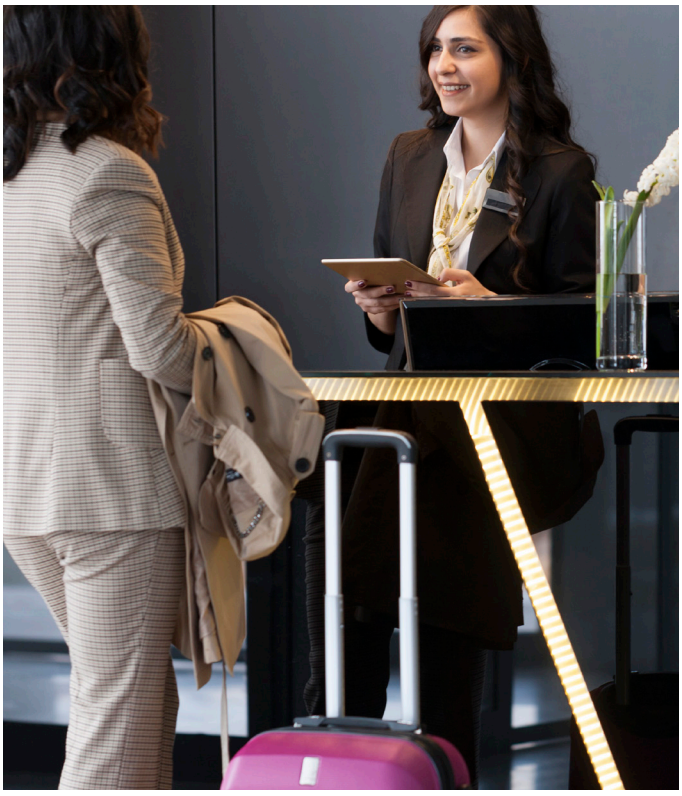
Accor wählt Verizon als Partner für die PCI Compliance

Lesen Sie, wie es der Hotelkette in Zusammenarbeit mit Verizon gelang, die teils komplexen Vorgaben des Payment Card Industry Data Security Standard (PCI DSS) zu erfüllen.

Herausforderung

Accor Gruppe: 5.400 Hotels, 10.000 Bars und Restaurants, 200 Millionen Mahlzeiten pro Jahr, 185.000 Besprechungs- und Arbeitsräume in 110 Ländern.

Als eine der führenden Hotelketten weltweit zählt die Accor Gruppe auf ihre 290.000 Mitarbeitenden und auf eine geschickte Kombination aus Zentralisierung und Autonomie in der Organisationsstruktur, um ihr Versprechen „hervorragende Erlebnisse zu bieten“ zu halten. „Wir benötigen mehrere verschiedene Ansätze, um in unseren teils sehr verschiedenartigen Etablissements überall dasselbe Maß an Sicherheit und Compliance zu gewährleisten,“ erklärt Marie-Christine Vittet, VP Compliance von Accor.



Die Accor Gruppe umfasst mehr als 40 Marken, die in zwei Kategorien (Luxury und Lifestyle einerseits und Premium, Midscale und Economy andererseits) zusammengefasst sind und das gesamte Spektrum von Touristen über Geschäftsreisende bis hin zu Telearbeitenden abdecken. „Accor berücksichtigt die Zahlungsgewohnheiten jeder Kundengruppe in jedem Land.“

Dennoch müssen all diese verschiedenen Kundenerlebnisse und -gewohnheiten mit denselben Sicherheits- und Compliancevorgaben in Übereinstimmung gebracht werden. Deshalb hat Accor seit 2008 eine Reihe von Initiativen durchgeführt, um Bezahlvorgänge und sein IT-System besser zu schützen. Im Jahr 2012 beschloss Accor, noch einen Schritt weiterzugehen und den PCI-DSS-Standard umzusetzen.

> **„Bei der Umsetzung unseres Complianceprogramms wollten wir die intellektuelle Agilität unserer Teams nutzen, bei technischen Fragen aber keine Kompromisse eingehen. Also haben wir eine Reihe von Standards und Prozeduren genutzt, um den Gästen in unseren sehr verschiedenen Umgebungen einen hervorragenden Service zu bieten.“**
>
> **Marie-Christine Vittet,**
> VP Compliance – Accor

verizon business

Lösung

Marie-Christine Vittet war für die Koordination aller PCI-DSS-Projekte in der Accor Gruppe verantwortlich und beschloss, die IT-Beratungsdienste von Verizon in Anspruch zu nehmen. Sie beschreibt, wie sie und ihre Teams die Voraussetzungen für die Compliance mit PCI DSS 2.0 schufen: „Die Expertise und Unterstützung von Verizon – einem Partner, mit dem wir bereits zusammengearbeitet hatten, – erschien uns eine solide Basis für die richtige Interpretation des Standards und die Entwicklung unserer eigenen PCI-DSS-Roadmaps, die auf einem Dokument namens ‚Prioritised Approach' basieren sollten."

Eine Arbeitsgruppe wurde geschaffen, um das Projekt über drei Jahre hinweg zu steuern. „Wir haben uns auf eine ambitionierte Roadmap geeinigt und Indikatoren definiert, um bei einem anspruchsvollen Projekt, das ohne die Unterstützung der IT-Teams nicht möglich wäre, auf Kurs zu bleiben."

Die Leitprinzipien für den gewählten Ansatz waren Transparenz und der Wille, dem Projekt einen echten Sinn zu geben. Zu dieser Zeit begannen Kreditkarten, Schecks und Bargeld als meistgenutzte Zahlungsmethode in Hotels abzulösen. Marie-Christine Vittet führt aus: „Die Begrüßung bei der Ankunft und die Bezahlung sind Schlüsselmomente für das Kundenerlebnis in all unseren Etablissements."

„Sichere, zuverlässige Zahlvorgänge sind daher eine wichtige Komponente des Willkommens, das wir als Accor Gruppe unseren Gästen bieten. Mit PCI DSS haben wir alte Praktiken, wie das Scannen beider Seiten einer Kreditkarte, abgelöst."

Ergebnisse

Im Jahr 2015 bewarb Accor sich nach dreijähriger harter Arbeit erstmals um eine PCI-DSS-Zertifizierung. „Die Bemühungen der Teams und Experten von Verizon zahlten sich aus, wir haben unsere erste Zertifizierung erhalten. Systemänderungen, Umgewöhnungen bei der Nutzung und beim Verhalten, technologische und finanzielle Investitionen – die Umstellung war tiefgreifend und trug zur Entstehung einer Complianceabteilung in der Accor Gruppe bei."

„Diese organisatorische Änderung war wichtig, weil wir dadurch gezeigt haben, welche Bedeutung die Compliance für all unsere Mitarbeitenden und Partner hat," betont Marie-Christine Vittet.

> **„Die Teams von Verizon spielten bei allen Projektetappen eine entscheidende Rolle. Sie standen uns als Berater und Partner zur Seite. Wir haben uns für Verizon entschieden, weil es einer von wenigen Anbietern mit einem eigenen PCI-DSS-Complianceprogramm war. Diese Partnerschaft hat beide Seiten gestärkt."**
>
> **Marie-Christine Vittet,**
> VP Compliance – Accor

verizon business

Vorteile

Partner, die zuhören und sich anpassen

Aufgrund ihrer Größe, ihrer internationalen Reichweite und ihrer hohen Standards benötigt die Accor Gruppe „Partner, die uns zuhören und sich auf uns einstellen“. „Da Verizon seine Services international bereitstellt, können die Teams dort besser verstehen, mit welchen Herausforderungen wir zu kämpfen haben. Zudem wissen wir zu schätzen, dass die QSAs (Qualified Security Assessors) mehrere Sprachen sprechen und sehr anpassungsfähig sind.“

Dies sind nur einige der spezifischen Features, die Accor beim Erreichen der PCI-Compliance geholfen haben. „Wir sind ständig bemüht, hohe Anforderungen an uns selbst zu stellen. Im Moment konzentrieren wir uns dabei auf die bevorstehende Einführung von PCI DSS 4.0.“

Anhaltender Support

Accor führt regelmäßig Audits durch, um für kontinuierliche Compliance mit dem PCI-DSS-Standard zu sorgen. Die Vorbereitung für diese Audits ist mit sechs Monaten Arbeitsaufwand für die verantwortlichen Teams verbunden. „Wir führen gern ein Vor-Audit durch, um uns auf das endgültige Audit vorzubereiten.“

„Dabei können wir überprüfen, was wir gelernt haben, und Bereiche mit Verbesserungsbedarf identifizieren.“ Nach diesem Vor-Audit können die identifizierten Verbesserungsmaßnahmen implementiert werden, bevor das eigentliche, bis zu drei Monate lange PCI-DSS-Audit beginnt. Im Rahmen dieses Audits werden über 50 Interviews durchgeführt, wozu Vertreter und Vertreterinnen vieler verschiedener Teams an wöchentlichen Besprechungen teilnehmen müssen.

„Dadurch entsteht eine niederschwellige, aber kontinuierliche Anspannung, die uns in die Lage versetzt, unser Compliancezertifkat und den dazugehörigen Compliancebericht (Report of Compliance, ROC) zu erhalten.“ Dieser Bericht wird dann an die Abteilung Quality Assurance von Verizon weitergeleitet, die das endgültige PCI-DSS-Zertifikat ausstellt.

Zukunftspläne

Der PCI-DSS-Standard wird weiterentwickelt und die Accor Gruppe plant, 2024 die Vorgaben von PCI DSS 4.0 zu erfüllen. Dazu hat die Hotelkette ein Komitee gegründet, das seinerseits einen Sharepoint erstellt hat, um die Erledigung der anstehenden Aufgaben zu koordinieren und die dabei vorgenommenen Verbesserungen regelmäßig zu kommunizieren. „In PCI DSS 4.0 gibt es die Dimension ‚Aktionsplanung‘. Diese nutzen wir bereits, um unser Versprechen, ein hervorragendes Erlebnis zu bieten, einzuhalten.“

Weitere Informationen:
PCI-Compliance

verizon business