Payment Card Industry Data Security Standard

Einleitung

Wer in einem Ladengeschäft oder bei einem Online-Shop einkauft und mit Kreditkarte bezahlt, vertraut darauf, dass mit den hierfür benötigten Kreditkartendaten sorgsam umgegangen wird. Damit bei allen Kreditkartenzahlungen einheitliche Mindestanforderungen zum Schutz der Karteninhaber gelten, gibt es den Payment Card Industry Data Security Standard, kurz PCI-Standard.

Alle Unternehmen, die im Endkundengeschäft tätig sind und die Kreditkarte als Zahlungsmittel akzeptieren, sollten daher schon einmal von dem PCI-Standard gehört und sich mit den Vorgaben vertraut gemacht haben. Dies gilt auch dann, wenn für die Zahlungsabwicklung ein Dienstleister beauftragt ist. Bei dieser Konstellation findet der PCI-Standard ebenfalls Anwendung, wobei der Auftraggeber für dessen Einhaltung verantwortlich bleibt und letztlich den Dienstleister insoweit kontrollieren muss.

Welche Bedeutung hat der PCI-Standard?

Bei dem PCI-Standard handelt es sich um ein Regelwerk, das maßgeblich von den Kreditkartenunternehmen erarbeitet wurde, um einen Missbrauch von Kreditkartendaten zu verhindern und damit auch die Einstandspflicht der Kreditkartenunternehmen zu reduzieren.

Über den PCI-Standard bestimmt das PCI Security Standards Council. Das PCI Security Standards Council ist eine in Delaware, USA zugelassene Limited Liability Corporation, die ursprünglich von American Express, Discover Financial Services, JCB International, MasterCard und Visa Inc. gegründet wurde. Neben den Kreditkartenunternehmen als Gründungsmitgliedern gehören mittlerweile auch weitere Unternehmen dem PCI Security Standards Council an, so dass es sich um ein offenes Forum für Unternehmen handelt, die mit der Abwicklung von Kreditkartenzahlungen befasst sind.

Wer muss die Anforderungen des PCI-Standards erfüllen?

Alle Unternehmen, die Kreditkarten akzeptieren, müssen sich dem PCI-Standard unterwerfen. Die Pflicht, den PCI-Standard einzuhalten, ergibt sich aus den Verträgen der Kreditkartenunternehmen mit den Händlern, die Kreditkarten akzeptieren. In den entsprechenden vertraglichen Klauseln, die von allen großen Kreditkartenunternehmen verwendet werden, wird dem Händler nur dann erlaubt eine Bezahlung per Kreditkarte zu akzeptieren, wenn der Händler den PCI-Standard einhält und dies auch nachweist.

Es sind allerdings nicht nur Händler von den Vorgaben des PCI-Standards betroffen. Auch Dienstleister, die für Händler tätig werden und dabei in den Kontakt mit Kreditkartendaten kommen, müssen nachweisen, dass der PCI-Standard von ihnen erfüllt wird. Dies folgt daraus, dass die Händler im Rahmen der zwölf Anforderungen des PCI-Standards auch sicherstellen müssen, dass von ihnen eingesetzte Dienstleister Kreditkartendaten nicht unerlaubt speichern. Händler müssen daher gegenüber ihren Dienstleistern die Verpflichtung zur Einhaltung des PCI-Standards weiterreichen. Dies gilt beispielsweise auch für Softwareunternehmen, die Kassensoftware anbieten, oder Lieferanten von Kassensystemen.

Zusätzlich zu einer ausdrücklichen Verpflichtung in einem Vertrag kann der PCI-Standard auch über die Auslegung von Generalklauseln in einen Vertrag einbezogen werden. Insoweit kann beispielsweise eine Klausel, die auf eine Leistungserbringung „nach dem Stand der Technik“ abstellt, die Pflicht zur Beachtung des PCI-Standards beinhalten, da es sich insoweit um branchenübliche Anforderungen handelt.

Wie wird die Einhaltung des PCI-Standards nachgewiesen?

Zum Nachweis der Einhaltung des PCI-Standards ist eine Zertifizierung vorgesehen, die von hierfür vom PCI Security

Standards Council zugelassenen Prüfern erfolgen kann. Diese werden mit der Überprüfung beauftragt und stellen bei positiver Prüfung ein entsprechendes Zertifikat aus. Grundlage der Prüfung sind dabei vordefinierte Untersuchungen und standardisierte Fragebögen. Alternativ kann die Zertifizierung teilweise auch über einen Fragebogen zur Selbsteinschätzung (Self-Assessment Questionaire) erfolgen.

Welche Anforderungen stellt der PCI-Standard an die Unternehmen?

Der PCI-Standard beschreibt verschiedene technische und organisatorische Maßnahmen, die von einem Händler und seinen Dienstleistern zu erfüllen sind. Thematisiert werden unter anderem die Installation und Einstellung einer Firewall, die verschlüsselte Übertragung von Kreditkartendaten und die Pflege der IT-Systeme. Um die jeweiligen Anforderungen zu erfüllen, muss ein Unternehmen nachweisen, dass ein lückenloser Schutz gewährleistet ist. Zu diesem Zweck werden die im Unternehmen getroffenen Maßnahmen im Rahmen einer Überprüfung intensiv hinterfragt. Abhängig davon, wie Kreditkartendaten im Unternehmen erhoben und verarbeitet werden, müssen so bis zu 329 Unterkriterien erfüllt werden, um die Einhaltung des PCI-Standards nachzuweisen. Diese Unterkriterien betreffen z.B. die physische Sicherung der Netzwerkbuchsen vor Zugriff durch Dritte und die Überprüfung von Systemprotokollen auf verdächtige Aktivitäten und Unregelmäßigkeiten.

Welche Folgen hat eine fehlende Beachtung des PCI-Standards?

Im PCI-Standard selbst sind keine Konsequenzen für den Fall vorgesehen, dass die Vorgaben des PCI-Standards missachtet werden. Die rechtlichen Konsequenzen richten sich vielmehr nach dem Vertragsverhältnis, mit dem die Einhaltung des PCI-Standards vereinbart wurde.

Je nach Inhalt des abgeschlossenen Vertrages können Kreditkartenunternehmen bei schwerwiegenden Verstößen des Händlers die weitere Akzeptanz von Kreditkartenzahlungen insgesamt untersagen. Dies hätte für den Händler zur Folge, dass er nicht mehr in Lage wäre, seinen Kunden die Zahlung mittels Kreditkarte anzubieten. Aus der Perspektive des Händlers ist dabei zu beachten, dass diesem gegenüber den Kreditkartenunternehmen auch das Verschulden von beauftragten Dienstleistern zugerechnet wird. Der Händler kann sich daher nicht darauf berufen, dass von ihm selbst alle Vorgaben eingehalten wurden und nur ein Dienstleister vertragswidrig mit Kreditkartendaten umgegangen ist. Den Ausführungen des PCI Security Standards Council lässt sich auch entnehmen, dass die Kreditkartenunternehmen Strafzahlungen für den Fall vorsehen, dass ein Händler die Vorgaben des PCI-Standards nicht erfüllt.

Außerdem kann ein Verstoß gegen den PCI-Standard dazu führen, dass ein Händler bei der Überprüfung nach dem PCI-Standard schlechter eingestuft wird und daher zukünftig genauere Nachweise zu erbringen oder häufigere Prüfungen vorzunehmen hat. Eine andere Eingruppierung aufgrund von Verstößen gegen den PCI-Standard führt dabei zwangsläufig auch zu höheren Kosten.

Schließlich wird darauf hingewiesen, dass jedenfalls bei Bekanntwerden eines Verstoßes gegen den PCI-Standard das Ansehen des Händlers in der Öffentlichkeit und gegenüber den Kreditkartenunternehmen erheblichen Schaden nehmen kann. Nach den gesetzlichen Bestimmungen gem. § 42a BDSG muss jeder Verlust von Kreditkartendaten unbedingt der Aufsichtsbehörde und den Betroffenen gemeldet werden. Stellt sich dabei heraus, dass der PCI-Standard nicht eingehalten wurde und deshalb die Daten missbraucht werden konnten, drohen zusätzlich Sanktionen der Aufsichtsbehörde und Schadensersatzansprüche der Betroffenen.

Fazit: Wie sollte sich ein Händler/Dienstleister verhalten?

Alle Unternehmen, die selbst Kreditkarten – sei es in einem Ladengeschäft oder im Online-Shop – akzeptieren, sollten unbedingt prüfen, ob eine Überprüfung der PCI-Standards schon einmal erfolgt ist. Soweit die Zahlungsabwicklung an einen Dienstleister vergeben wurde, sollte der entsprechende Vertrag unbedingt darauf überprüft werden, ob sich in dem Vertrag Aussagen zum PCI-Standard und einer Zertifizierung nach dem PCI-Standard finden. Hier geht es vor allem um die Frage, wer im Innenverhältnis für das Thema zuständig ist.

Alle Unternehmen, die im Umfeld von Händlern selbst als Dienstleister oder Partner tätig sind, müssen genauer prüfen, ob auch sie dem PCI-Standard unterfallen und welche Konsequenzen dies für ihre Dienstleistungen hat.

Robert Bommel, BRANDI Rechtsanwälte I robert.bommel@brandi.net

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Datenschutzauditor (TÜV)

Adenauerplatz 1
33602 Bielefeld
Tel.: +49 (0) 521 / 96535 – 812
Fax: +49 (0) 521 / 96535 – 115
Mail: sebastian.meyer@brandi.net
Web: www.brandi.net