Vorgelegt durch:
Patrick Sauer

M.- Nr. : 2010XXXX

Hausarbeit

- Sicherheitsstandards zur sicheren Zahlung-

Übersicht über die internationalen, europäischen und nationalen Standards zur Sicherung von elektronischen Zahlungen sowie die Bewertung der Regelungen nach Verbindlichkeit und Freiwilligkeit.

FH Brandenburg / University of applied sciences

Version 1.0

Inhaltsverzeichnis

1 Einleitung und Zielsetzung ..... - 1 -

2 Zahlungsarten im Internet ..... - 2 -

2.1 Kreditkarte ..... - 2 -

2.1.1 Einführung ..... - 2 -

2.1.2 Rechtsverhältnis zwischen Kartenemittent und Vertragsunternehmen ..... - 4 -

2.1.3 Rechtsverhältnis zwischen Karteninhaber und Kartenemittent ..... - 4 -

2.1.4 Risiko bei MOTO-Transaktionen ..... - 5 -

2.1.5 MasterCard SecureCode und Verified by VISA ..... - 5 -

2.1.6 Anforderungen aus dem KWG und der BaFin ..... - 5 -

2.1.7 Risikoverteilung und Sicherheitsziele ..... - 6 -

2.1.8 Bundesdatenschutzgesetz ..... - 7 -

2.2 Lastschrift ..... - 8 -

2.2.1 Einführung ..... - 8 -

2.2.2 Rechtsverhältnis zwischen Gläubiger und seiner Bank ..... - 8 -

2.2.3 Rechtsverhältnis zwischen Schuldner und seiner Bank ..... - 9 -

2.2.4 Risiken und Schutzziele beim Einzugsermächtigungsverfahren ..... - 10 -

2.2.5 Anforderungen aus dem KWG und der BaFin ..... - 10 -

2.2.6 Bundesdatenschutzgesetz ..... - 12 -

3 Sicherheitsstandards ..... - 13 -

3.1 Sicherheitsziele und Einführung ..... - 13 -

3.2 ISO 27000-Serie ..... - 13 -

3.2.1 ISO 27001 ..... - 14 -

3.2.2 ISO 27002 und ISO 27015 ..... - 15 -

3.3 Payment Card Data Security Standard (PCI DSS) ..... - 15 -

3.3.1 Sicherheitsziele ..... - 15 -

3.3.2 Organisatrionsstruktur ..... - 16 -

3.3.3 Zertifizierung ..... - 17 -

3.3.4 Kritische Betrachtung mit europäischem Recht ..... - 17 -

4 Fazit ..... - 19 -

5 Anhang I. Literaturverzeichnis ..... - 20 -

1 Einleitung und Zielsetzung

Diese Hausarbeit soll einen kurzen Überblick über die verschiedenen elektronischen Zahlungsarten geben und die rechtliche Situation beurteilen. Hierbei soll insbesondere herausgearbeitet werden, welche rechtlichen Risiken bzw. Haftungsrisiken für die verschiedenen Parteien existieren und welche Sicherheitsziele sich daraus ergeben.

Danach sollen die relevanten Sicherheitsstandards dargestellt werden, die für das Erreichen der zuvor ausgearbeiteten Sicherheitsziele relevant sind. Diese sollen dahingehend analysiert und bewertet werden, ob die Einhaltung bzw. eine Zertifizierung nach dem Standard für ein Unternehmen eine Haftungsbegrenzung oder eine Haftungsprivilegierung erreichen kann.

Abschließend soll bewertet werden, ob die Einhaltung von Standards verbindlich vorgeschrieben werden kann. Hierbei ist zwischen der Inbezugnahme des Staates auf Normen und der defacto-Verbindlichkeit von privaten Standards zu unterscheiden. Weiter sollen eventuelle rechtliche Konflikte mit dem Wettbewerbsrecht besprochen werden, die sich durch den Zwang privater Standards ergeben.

2 Zahlungsarten im Internet

Oftmals stehen Kunden in Onlineshops verschiedene Zahlungsarten zur Verfügung. Dies kann unter anderen folgenden Varianten erfassen:

- Überweise und damit Vorkasse
- Lastschrifteinzug
- Kreditkarte
- Nachnahme
- Alternative Zahlungsdienste (z.B. Paypal)

Bei der klassischen Überweisung oder Nachnahme werden vom Käufer keine Angaben über persönliche Zahlungsdaten wie z.B. der Kontonummer getätigt. Die Alternativen Zahlungsmethoden wie z.B. Paypal reduzieren sich am Ende der Zahlungskette wieder auf das Lastschriftverfahren oder die Kreditkartenzahlung. Nachfolgend wird demnach nur die rechtliche Ausgestaltung von den beiden Zahlungsarten und die Besonderheiten bzgl. des Einsatzes im Internet analysiert.

2.1 Kreditkarte

2.1.1 Einführung

Die Kreditkarte stammt ursprünglich aus den USA und wurde 1894 erstmals als Kundenkreditkarte von einem Unternehmen herausgegeben. Mittlerweile werden hauptsächlich sogenannte Universalkarten benutzt, die eine Zahlung beim verschiedenen Händler ermöglicht.[1] In Deutschland sind Karten von VISA und MasterCard sowie AmericanExpress die bekanntesten Kreditkarten-Typen.[2] Die Abrechnung einer Karte selbst kann unterschiedlich ausgeprägt sein. So gibt es Karten, deren aufsummierte Zahlungsbeträge monatlich dem Karteninhaber in Rechnung gestellt und teilweise auch klassisch als Ratenzahlung (Verbraucherdarlehen nach §491 BGB[3]) abgezahlt werden. Auf der anderen Seite existieren auch Guthabenkarten oder Karten, bei denen durch einen Zahlungsvorgang ein Girokonto bei einer Bank direkt belastet wird.[4]

Kreditkarten stellen nicht nur in der realen Welt einen bequemen und sicheren Zahlungsweg da, sondern werden auch im Internet als Zahlungsmittel eingesetzt und vereinfachen dort den grenzüberschreitenden Handel bzw. Zahlungsverkehr.[5] Neben verschiedenen wirtschaftlichen Funktionen der Kreditkarte (z.B. universales Zahlungsmittel, Bargeldbeschaffung, Kreditgewährung) wird nachfolgend nur auf die

---

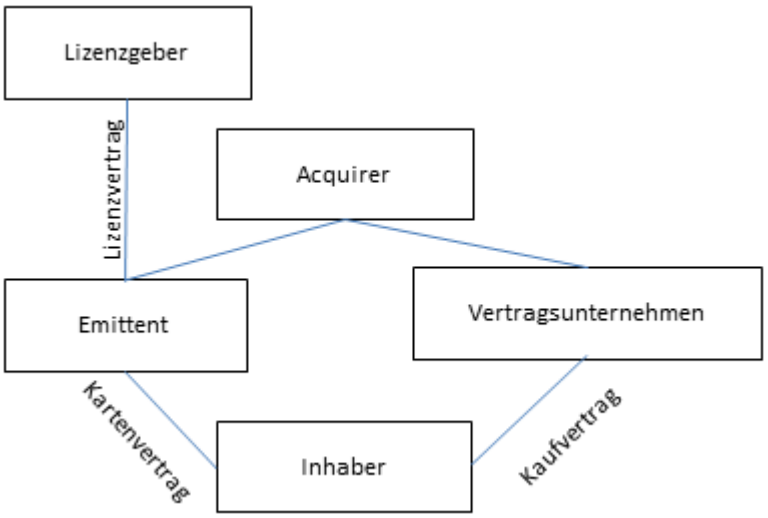
[1] Vgl. [Nitsch], Seite 114.
[2] Vgl. [Nitsch], Seite 115.
[3] Bürgerliches Gesetzbuch. In der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, ber. S. 2909, 2003 I S. 738) zuletzt geändert durch Gesetz vom 27.07.2011 (BGBl. I S. 1600) m.W.v. 04.08.2011
[4] Vgl. [Nitsch], Seite 115.
[5] Vgl. [Kümpel], Seite 1120.

Funktion als Zahlungsmittel im Internet eingegangen. Diese Transaktionen werden als MOTO (Mailorder/Telephonorder) klassifiziert[6]. Bei diesen Transaktionen liegt weder ein unterschriebener Beleg vor, noch eine Validierung durch die persönliche und geheime PIN eines Karteninhabers.

Die Herausgabe von Kreditkarten sowie deren Verwaltung ist kein Bankgeschäft im Sinne des §1 Abs. 1 KWG[7], sodass Unternehmen mit diesen Geschäftsmodellen keine Banken sind. Nach §1 Abs. 3 KWG zählen sie jedoch zu den Finanzinstituten.[8] Des Weiteren ist für die Kreditkartenausgabe und –abrechnung eine Erlaubnis der BaFin erforderlich (§8 Abs. 1 ZAG), da nach §1 Abs. 2 Nr. 4 ZAG dies zu den Zahlungsdiensten zählt.[9]

Das Kreditkartengeschäft der heutigen Universalkreditkarten von VISA und MasterCard basiert auf einem sogenannten Mehrparteienrechtsverhältnis und beinhaltet maximal folgende Parteien:[10]

- Einem Lizenzgeber, z.B. VISA oder MasterCard,
- einem Kartenemittent (‚Issuer'),
- einer Abrechungsstelle (‚Acquirer'),
- einem Vertragsunternehmen (Shop) sowie
- einem Karteninhaber



Bei der Kreditkartenabwicklung im Internet wird diese Konstellation oftmals noch durch einen oder mehreren „Internet Payment Service Provider" ergänzt, die sich zwischen

---

[6] Vgl. [Nitsch], Seite 117.
[7] Gesetz über das Kreditwesen. Neugefasst durch Bek. v. 9.9.1998 I 2776; zuletzt geändert durch Art. 2 Abs. 72 G v. 22.12.2011 I 3044
[8] Vgl. [Nitsch], Seite 115.
[9] Vgl. [Einsele], Seite 303.
[10] Vgl. [Einsele], Seite 305f.

einem Onlineshop und einem Acquirer positionieren und Zahlungen weiterleiten. Zur Vereinfachung wird bei der rechtlichen Betrachtung des Kreditkartengeschäfts von einem 3-Parteien-System zwischen Karteninhaber, Kartenemittent und Vertragsunternehmen ausgegangen.

2.1.2 Rechtsverhältnis zwischen Kartenemittent und Vertragsunternehmen

Zwischen den Kartenemittenten und Vertragsunternehmen wird ein sogenannter Akquisitionsvertrag geschlossen. Durch die damit verbundene Verpflichtung des Vertragsunternehmen Zahlungen per Kreditkarte anzunehmen, handelt es sich hierbei um einen Vertrag zugunsten Dritter (§328 BGB).[11] Dieser Vertrag regelt unter anderem das Disagio bei Zahlungen, welches eine Reduktion der Forderung ist, der der Emittent einhalten darf. [12] Des Weiteren wird die Höchstgrenze von Beträgen, sowie insbesondere die Verpflichtung des Emittenten die Zahlungen des Karteninhabers auszugleichen, geregelt. Dies betrifft auch die in der Einführung erwähnten MOTO-Transaktionen, auch wenn dort kein Beleg bzw. keine Unterschrift vorliegt. Eventuelle Klauseln für Rücklastschriften, falls der Kunde eine Forderung im MOTO-Verfahren nicht anerkennt, sind laut Nitsche nach deutscher Rechtsprechung vom BGH[13] als ungültig anzusehen.[14]

2.1.3 Rechtsverhältnis zwischen Karteninhaber und Kartenemittent

Der zwischen Karteninhaber und Kartenemittent geschlossener Vertrag wird als Emissionsvertrag bezeichnet. Dies ist ein Geschäftsbesorgungsvertag (§675 BGB) bei diesem sich der Emittent verpflichtet, alle vom Karteninhaber eingegangen Zahlungsverpflichtungen zu erfüllen. Der Karteninhaber erkennt die Forderungen des Emittenten nach §781 an (abstraktes Schuldverhältnis). Durch das Nennen seiner Kreditkartennummer weist der Karteninhaber über das Vertragsunternehmen den Emittenten an, die entstehenden Forderungen des Vertragsunternehmens zu erfüllen. Hierbei entsteht ein Erstattungsanspruch des Emittenten gegenüber dem Karteninhaber (§675 und §670 BGB). Grundsätzlich ist der Emittent in der Verpflichtung, seine Forderungen gegenüber dem Karteninhaber nachweisen zu können. Dies kann bei MOTO-Transaktionen aufgrund fehlender Unterschrift nicht realisiert werden.[15]

---

[11] Vgl. [Nitsch], Seite 116.
[12] Vgl. [Nitsch], Seite 116.
[13] BGH 12.07.2005, WM 2005, 1601, 1602.
[14] Vgl. [Nitsch], Seite 116f.
[15] Vgl. [Nitsch], Seite 117f.

2.1.4 Risiko bei MOTO-Transaktionen

Durch den nicht vorhandenen Weisungsbeleg bei MOTO-Transaktionen im Internet ist diese Zahlungsart sehr missbrauchsanfällig[16]. Wie zuvor dargelegt, trägt hierbei das Risiko der Kartenemittent und nicht der Karteninhaber. Dies führt dazu, dass aus Sicht der Kartenemittenten die Vertraulichkeit von einer Kreditkartennummer ein hohes Sicherheitsziel sein muss, um den Missbrauch bei MOTO-Transaktionen begrenzen zu können. Dem erklärten Ziel des Schutzes im Sinne der Vertraulichkeit der Karteninhaberdaten widmet sich der nachfolgend noch erläuterte ‚Payment Card Data Security Standard'.

2.1.5 MasterCard SecureCode und Verified by VISA

Um den Missbrauch bei MOTO-Transaktionen zu reduzieren, wurde der Zahlungsprozess bei MOTO-Transaktionen um einen zusätzlichen Credential des Karteninhabers erweitert. Bei diesen sogenannten 3D-Authorisierungen (MasterCard SecureCode und Verified by VISA) legt der Karteninhaber ein geheimes persönliches Passwort fest. Besitzt er nun eine Kreditkarte mit 3D-Unterstützung und bietet das Vertragsunternehmen als Internethändler diese Technik an, muss der Kunde eine mögliche Zahlung mit seinem geheimen Passwort bestätigen. Andernfalls ist eine Zahlung per Kreditkarte nicht möglich.[17] Somit ist es für einen Kartenemittenten nun möglich, eine Weisung des Karteninhabers bei Zahlungen im Internet besser nachweisen zu können.

2.1.6 Anforderungen aus dem KWG und der BaFin

Nachdem die reine Herausgabe und Verwaltung von Kreditkarten keine Bankgeschäfte sind und diese Unternehmen nur zu den Finanzinstituten zählen[18], gelten für diese nicht die besonderen organisatorischen Pflichten (nach §25a KWG) wie für Institute (nach §1 Abs. 1b KWG) und sie unterliegen auch nicht der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (§6a KWG). Dies ändert sich für Kreditkatenemittenten, wenn die Herausgabe von Kreditkarten mit zusätzlichen Bankgeschäften z.B. Gelddarlehen (nach §1 Abs. 1 KWG) kombiniert wird. In diesem Fall gelten die in Kapitel 2.2.5 dargestellten Anforderungen aus dem KWG und der BaFin.

---

[16] Vgl. [Kümpel], Seite 1127.
[17] Vgl. auch [Chen], Seite 80.
[18] Vgl. Kapitel 2.1.1.

2.1.7 Risikoverteilung und Sicherheitsziele

Beim Kartenemittent sind die meisten und gewichtigsten Risiken versammelt. Er hat nicht nur das Zahlungsausfallsrisiko aufgrund mangelnder Bonität des Karteninhabers, sondern auch das Missbrauchsrisiko zu tragen. Aus der Sicht der Informationssicherheit ergibt sich hier das Ziel der Vertraulichkeit der gesamten Karteninhaberdaten, um den möglich Missbrauch einzugrenzen. Das Zahlungsausfallsrisiko kann er durch eine risikoorientierte Auswahl von Karteninhabern als Kunden steuern. Durch die gesetzlichen Anforderungen einer korrekten Buchführung sowie den Bedarf auf diese Informationen regelmäßig und automatisiert zuzugreifen, sind die Informationsziele der Integrität (inkl. Nachvollziehbarkeit) und Verfügbarkeit zu berücksichtigen.

Die Abrechnungsstellen und Vertragsunternehmen besitzen die gleichen Risiken. Da die Zahlung des Karteninhabers durch den Emittenten garantiert wird, ergibt sich kein Ausfallrisiko. Da beide Karteninhaberdaten verarbeiten, werden Ihnen vom Emittenten vertraglich festgelegte Strafzahlungen sowie Haftungsrisiken auferlegt, sofern bei Ihnen Karteninhaberdaten gestohlen werden.[19] Somit ergibt sich auch für diese das Ziel der Vertraulichkeit der kompletten Karteninhaberdaten. Die Ziele Integrität und Verfügbarkeit sind analog des Kartenemittenten vorhanden.

Für den Karteninhaber ist die Zahlung mit seiner Kreditkarte selbst risikolos. Er trägt jedoch grundsätzlich ein Haftungsrisiko in der Höhe von maximal 150€ (§675 v BGB), sofern die Authentifizierungsdaten abhandenkommen.[20] Hierbei ist zu beachten, dass bei MOTO-Transaktionen gar keine Authentifizierungsdaten übermittelt werden und somit auch nicht abhandenkommen können. Dies bedeutet, dass der Verlust/Diebstahl der reinen Kreditkartennummer zwar Missbrauch (per MOTO-Transaktion) zulässt, der Karteninhaber dafür aber nicht haftet. Dieser Sachverhalt ändert sich bei Online-Zahlungen, die um eine 3D-Authentisisierung erweitert werden. Hierbei wird wieder ein geheimes und persönliches Credential zur Autorisierung eingesetzt. Als Sicherheitsziel tritt hier die Vertraulichkeit der Autorisierungsdaten für den Karteninhaber in den Vordergrund.

Der Lizenzgeber trägt im gesamten Zahlungsprozess weder Haftungs- noch Missbrauchsrisiken. Sein Geschäftsmodell jedoch ist davon abhängig, dass Kreditkarten als sicheres Zahlungsmittel betrachtet werden, sodass für ihn der reine

---

[19] Vgl. [Bradley], Seite 26f.
[20] Vgl. [Kümpel], Seite 1139.

betriebswirtschaftliche Anreiz vorhanden ist, die Sicherheit und damit insbesondere die Vertraulichkeit der Karteninhaberdaten zu gewährleisten. Dieser Anreiz manifestiert sich in der Praxis im PCI DSS, der in Verbindung mit Strafzahlungen die gesamte Kreditkartenindustrie dazu bringen soll, die Vertraulichkeit der Karteninhaber zu gewährleisten.[21]

2.1.8 Bundesdatenschutzgesetz

Die Karteninhaberdaten (inkl. der Kreditkartennummern) sowie weitere Abrechnungsdaten über eine Karte sind personenbezogene Daten (nach §3 Abs.1 BDSG[22]), deren Schutz durch technische und organisatorische Maßnahmen zu gewährleisten ist (§9 BDSG).

Die Anlage zu §9 BDSG werden verschiedene Kontrollbereiche für die geforderten technischen und organisatorischen Maßnahmen aufgeführt:[23]

- Organisationskontrolle
- Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Datentrennungskontrolle

Diese Kontrollbereiche lassen sich auf die üblichen Sicherheitsziele[24] in der Informationsverarbeitung übertragen.[25] Das Bundesdatenschutzgesetz stellt keine technischen Vorschriften an die Datenverarbeitung und überlässt dem Unternehmen die Auswahl dieser. Bei der Auswahl der Maßnahmen wird eine Abwägung zwischen ihrem Aufwand und dem angestrebten Schutzzweck gefordert (§9 BDSG). Grundsätzlich sind Unternehmen bei einem Diebstahl bzw. Missbrauch der durch sie erhobenen und verarbeiteten Daten gegenüber einem Betroffenen schadensersatzpflichtig (§7 BDSG). Hierbei kann allerdings ein Haftungsprivileg erzielt werden, wenn das Unternehmen die notwendig Sorgfalt beachtet hat (§7 BDSG). Um die Anforderungen des §9 BDSG in Hinblick auf ein Haftungsprivileg zu erfüllen, muss ein Unternehmen die angemessene Auswahl von technischen und organisatorischen Maßnahmen nachweisen können. Dies kann zum Beispiel über die Durchführung einer Risikoanalyse auf Informationsbasis nach

---

[21] Kapitel 3.3.1:
[22] Bundesdatenschutzgesetz. Neugefasst durch Bek. v. 14.1.2003 I 66; Zuletzt geändert durch Art. 1 G v. 14.8.2009 I 2814.
[23] Vgl. [Witt], Seite 138f.
[24] Kapitel 3.1.
[25] Vgl. [Witt], Seite 141.

ISO 27005 erreicht werden,[26] welches ein Bestandteil eines Informationssicherheitsmanagementsystems nach ISO 27001 ist.

2.2 Lastschrift

2.2.1 Einführung

Beim Lastschriftverfahren wird im Gegensatz zu Überweisungen die Zahlung nicht von einem Schuldner, sondern von einem Gläubiger veranlasst. Den Auftrag zur Lastschrift übermittelt der Gläubiger seiner kontoführenden Bank. Die Bank des Gläubigers übermittelt die Lastschriftanweisung über evtl. andere Banken an die Bank des Schuldners. Diese belastet dann sein Konto und transferiert den angegeben Geldbetrag zur Bank des Gläubigers auf dessen Konto. Eine Lastschrift wird somit auch als ‚rückläufige Überweisung' bezeichnet.[27]

Im Lastschriftabkommen der Kreditwirtschaft werden zwei verschiedene Ausprägungen einer Lastschrift erläutert:

- Abbuchungsverfahren
- Einzugsermächtigungsverfahren

Beim Abbuchungsverfahren erteilt der Schuldner seiner Bank einen Auftrag (§675f Abs. 3 Satz 2 BGB), Abbuchungen von einem Gläubiger zu akzeptieren und sein Konto entsprechend zu belasten. Ist das Konto ausreichend gedeckt und die Lastschrift per Abbuchungsverfahren eingelöst, existiert kein weiteres Widerspruchsrecht des Schuldners bei einer Lastschrift des Gläubigers. Beim Einzugsermächtigungsverfahren hingegen erteilt der Schuldner nicht seiner Bank, sondern dem Gläubiger die Erlaubnis sein Konto per Lastschrift zu belasten. Im Gegensatz zum Abbuchungsverfahren gilt hierbei die Lastschrift nicht sofort als eingelöst und es existiert ein Widerspruchsrecht des Schuldners gegenüber seiner Bank.[28] Im Bereich der Zahlungsmöglichkeiten im Internet kommt primär das Einzugsermächtigungsverfahren zum Einsatz, sodass das Abbuchungsverfahren nicht weiter erläutert wird.

2.2.2 Rechtsverhältnis zwischen Gläubiger und seiner Bank

Der Gläubiger schließt mit seiner Bank eine Inkassovereinbarung. In dieser werden die Bedingungen für den Lastschrifteinzug geregelt. Da die Bank das Risiko des Zahlungsausfalles trägt, wenn ein Schuldner einer Lastschrift widerspricht und der Gläubiger über keine ausreichende Kontodeckung verfügt, wird eine Bank nur

---

[26] Vgl. auch [Witt], Seite 103.
[27] Vgl. [Kümpel], Seite 963.
[28] Vgl. [Kümpel], Seite 966f.

Inkassoverträge mit seriösen Kunden treffen, die eine ausreichende Bonität vorweisen können. Mit der Inkassovereinbarung verpflichtet sich der Gläubiger nur Lastschriften einzureichen, wenn er von dem Schuldner eine schriftliche Einwilligung besitzt. Hierbei kann es von der Bank verlangt werden, den Nachweis zu führen. Nach Ansicht des BGH ist es jedoch nicht erforderlich, dass eine Bank prüft, ob überhaupt eine Einzugsermächtigung erteilt wurde.[29]

Die Gutschrift eines Betrages erfolgt bei der Lastschrift auf dem Gläubigerkonto zwar sofort, jedoch nur unter Vorbehalt (§158 Abs. 1 BGB). Dieses Schuldversprechen (§780 BGB) steht unter der aufschiebenden Bedingung, dass die Bank des Schuldners die Lastschrift einlöst. Die Bank des Gläubigers trägt grundsätzlich das Risiko, dass die Lastschrift nicht eingelöst wird oder dass der Lastschrift vom Schuldner widersprochen wird. Da die Bank die Zahlung dem Gläubiger (und damit ihrem eignen Kunden) aber sofort gutschreibt, entstände ihr ein Schaden bei einer Zahlungsunfähigkeit des Schuldners. Zur Reduzierung eines möglichen Schadens gehen beim Einreichen der Lastschrift die damit zu begleichenden Forderungen des Gläubigers auf die Bank über (Nr. 15 Abs. 2 AGB-Privatbanken). Grundsätzlich sollte daher die Bank vor Abschluss von Inkassovereinbarungen ihre Kunden ausreichend prüfen und kann dadurch ihr Risiko beeinflussen.[30]

2.2.3 Rechtsverhältnis zwischen Schuldner und seiner Bank

Die Teilnahme am Lastschriftverfahren muss im Gegensatz zur Beauftragung nicht zusätzlich vereinbart werden, da sie bereits in seinen vertraglichen Vereinbarungen über das Girokonto enthalten sind[31]. Grundsätzlich gibt der Schuldner bei der Lastschrift im Einzugsermächtigungsverfahren seiner Bank keinen Auftrag, Geldbeträge von seinem Girokonto einzuziehen. Die Bank handelt somit ohne direkten Auftrag und auf eigene Rechnung. Der Schuldner kann aber die Belastung nachträglich genehmigen (§675j Abs. 1 BGB). Durch die Belastung ohne direkten Auftrag des Schuldners an die Bank, erwirbt dieser ein Widerspruchsrecht. Das Widerspruchsrecht besteht auch, wenn die Lastschrift berechtigt ist. Ein solcher Widerspruch muss die Bank des Schuldners dennoch anerkennen und eine Rücklastaschrift ausführen. Nach Ansicht des BGH ist das Widerspruchsrecht des Schuldners unbegrenzt gültig, solange er nicht der Lastschrift zugstimmt hat. Seine Bank selbst hingegen kann die Lastschrift nach dem Lastschriftabkommen (Abschnitt 3, Nr.1 und 2) nur innerhalb von sechs Wochen

---

[29] Vgl. [Kümpel], Seite 967f.
[30] Vgl. [Kümpel], Seite 969-971.
[31] Vgl. [Kümpel], Seite 972.

zurückgeben. Die Genehmigung der Lastschrift kann stillschweigend vereinbart werden und liegt mit dem Verstreichen einer sechswöchigen Frist nach Rechnungsabschluss vor.[32]

2.2.4 Risiken und Schutzziele beim Einzugsermächtigungsverfahren

Für den Kunden selbst ist das Einzugsermächtigungsverfahren aufgrund seines umfangreichen Widerspruchrechts risikolos. Für die Bank eines Schuldners selbst besteht kein Risiko, sofern

- sie zeitnah innerhalb der Frist zwischen den Instituten die Genehmigung des Schuldners zur Lastschrift erhält und
- bei einer möglichen Rückbelastung die Bank des Gläubigers nicht zahlungsunfähig wird.

Das Risiko besteht somit auf der Gläubigerseite. Für den Gläubiger besteht ein Zahlungsausfallrisiko, indem die Lastschrift nicht erfolgreich ist oder dieser später widersprochen wird. Für Bank des Gläubigers besteht das Risiko, dass diese bei mangelnder Bonität Rücklastschriften gewähren muss, ohne dafür vom eigentlichen Gläubiger eine Erstattung zu bekommen. Dieses Risiko kann sie aber durch Auswahl ihrer Vertragspartner selbst steuern.
Im Gegensatz zu Kreditkartendaten ergeben sich hierbei keine gesteigerten Schutzziele im Bereich der Vertraulichkeit von Kontoinformationen.

2.2.5 Anforderungen aus dem KWG und der BaFin

Banken und Finanzdienstleister unterliegen aufgrund ihrer Relevanz für die Volkswirtschaft der Regulierung des Staates. Da Ausfälle der Informationstechnologie oder Fehler in der Informationsverarbeitung dieser Unternehmen volkswirtschaftliche Schäden verursachen können, unterliegt auch auch dieser Bereich der staatlichen Kontrolle.[33] Dies wird über das Kreditwirtschaftsgesetz und der Aufsicht der BaFin realisiert.[34]

Nachdem die Abwicklung von Überweisungen Kreditinstituten vorbehalten (§1 Abs. 1 KWG) ist, gelten somit für Kreditinstitute sowie Finanzdienstleistern (nach §1 Abs. 2 KWG als Institute bezeichnet) besonderen organisatorische Pflichten (§25a KWG). Diese beinhalten unter anderem die Durchführung und Kontrolle eines Risikomanagements

---

[32] Vgl. [Kümpel], Seite 979-985.
[33] Vgl. [Spindler-2], Seite 181.
[34] Vgl. [Spindler-2], Seite 182.

(§25a Abs. 1 KWG). Hierbei wird explizit auf ein Notfallkonzept für IT-Systeme (§25a Abs. 1 Punkt 3 KWG) und eine angemessene technisch-organisatorische Ausstattung (§25a Abs. 1 Punkt 2 KWG) verwiesen. Diese Angemessenheit muss sich grundsätzlich an den Zielen des Kreditwirtschaftsgesetzes orientieren.[35]

Die Bundesanstalt für Finanzdienstleistungsaufsicht ist seit dem 1. Mai 2002 die deutsche Allfinanzaufsicht und eine rechtsfähige Anstalt des öffentlichen Rechts (Art. 87 Abs. 3 Satz 1 GG[36]).[37] Es ist Aufgabe der BaFin möglichen Risiken entgegenzuwirken, die entweder die Durchführung von Bankgeschäften stören können oder Nachteile für die Gesamtwirtschaft bringen können (§6 Abs. 2 KWG). Konsequenterweise unterliegen Institute der Aufsicht dieser Bundesanstalt (§6 Abs. 1 KWG), wobei diese auch Anweisungen treffen kann, die für die Institute verbindlich sind (§6 Abs. 3 KWG). Dies beinhaltet auch die Konkretisierung der Anforderungen des §25a KWG.[38]

Mit den Mindestanforderungen an das Risikomanagement (MaRisk) hat die Bundesanstalt für Finanzdienstleistungsaufsicht die in §25a KWG genannten Anforderungen an ein Risikomanagement konkretisiert. Diese Mindestanforderungen werden per Rundschreiben veröffentlicht und sind für alle Institute als Anweisung der BaFin verbindlich. Neben konkreten Anforderungen an die Ausgestaltung des Risikomanagements, werden auch Anforderungen an die Informationssicherheit gestellt:

> *„Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen.“*[39]

Die MaRisk verweist explizit auf gängige Standards für die IT-Systeme und IT-Prozesse, um die zuvor aufgeführten Sicherheitsziele zu erreichen.[40] In den Erläuterungen der MaRisk[41] werden zwei Standards aufgeführt:[42]

- IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Internationaler Sicherheitsstandard ISO/IEC 2700x

---

[35] Vgl. [Spindler-2], Seite 185.
[36] Grundgesetz. Zuletzt geändert durch Art. 1 G v. 21.7.2010 I 944.
[37] Vgl. [Buck], Seite 283.
[38] Vgl. [Spindler-1], Seite 198.
[39] AT 7.2 Abs. 2 MaRisk. Rundschreiben 11/2010 (BA)
[40] Vgl. AT 7.2 Abs. 2 MaRisk
[41] Anlage 1: Erläuterungen zu den MaRisk in der Fassung vom 15.12.2010
[42] Vgl. AT 7.2 Erläuterungen zu den MaRisk, Seite 20

Der Verweis auf die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik ist hierbei kritisch zu bewerten. Das BSI ist nicht für die Sicherheit von Banken und Finanzdienstleistern im Allgemeinen zuständig, sondern primär nur für die IT-Sicherheit des Bundes (§3 BSIG[43]). Die Verlautbarungen des BSI in Form der IT-Grundschutzkataloge sind hierbei keine anerkannten Normen (insbesondere keine Norm des DIN e.V.) und entsprechen auch nicht den Anforderungen der Verordnung 315/2011 der europäischen Kommission, da die in Anhang II aufgeführten Voraussetzungen nicht erfüllt werden. Die Ansichten des BSI sind somit nur als Expertenmeinung zu bewerten, sodass durch die Einhaltung der BSI-Empfehlungen und auch eine Zertifizierung (ISO 27001 auf Basis von IT-Grundschutz) keine Haftungsprivilegien zu erreichen sind. Als weiterer Nachteil ist anzumerken, dass der BSI-Grundschutz aufgrund mangelnder Normung international nicht anerkannt ist. Somit ergeben sich für Banken und Finanzdienstleistern eine deutlich bessere Haftungsreduktion sowie eine bessere internationale Anerkennung einer Zertifizierung, wenn ein Informationssicherheitsmanagementsystem nach ISO 27001 betrieben wird als bei der Umsetzung bzw. einer Zertifizierung nach BSI Grundschutz.

2.2.6 Bundesdatenschutzgesetz

Kontoinformationen sowie die Überweisungsdaten selbst sind personenbezogene Daten (nach §3 Abs.1 BDSG[44]), deren Schutz durch technische und organisatorische Maßnahmen zu gewährleisten ist (§9 BDSG). Es gelten hierbei die in Kapitel 2.1.8 aufgeführten Anforderungen auch auf Kontoinformationen.

---

[43] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik. "BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821)."

[44] Bundesdatenschutzgesetz. Neugefasst durch Bek. v. 14.1.2003 I 66; Zuletzt geändert durch Art. 1 G v. 14.8.2009 I 2814.

3 Sicherheitsstandards

3.1 Sicherheitsziele und Einführung

Sicherheitsstandards im Bereich der Informationstechnologie oder Informations- und Kommunikationstechnik definieren konkrete Maßnahmen oder Managementmodelle zur Sicherstellung von einem oder mehreren Zielen der Informationssicherheit. In der Informationssicherheit sind dies in der klassischen Betrachtung,

- die Vertraulichkeit ,
- die Verfügbarkeit und
- die Integrität von Daten und Systemen. [45]

Diese können in der betrieblichen Praxis um weitere Ziele ergänz werden:[46]

- Die Verifizierung von Subjekten (Authentizität),
- die Nachvollziehbarkeit von Handlungen,
- sowie die Nicht-Abstreibarkeit von Handlungen.

Die nachfolgend vorgestellten Standards weisen verschiedene Intentionen und Zielgruppen auf. Manche definieren primär Prozesse (z.B. ISO 27001) und wenden sich sehr generisch an alle Unternehmen oder Institutionen. Andere hingegen haben nur eine begrenzte Zielgruppe und definieren eher technische und/oder organisatorische Sicherheitsmaßnahmen (z.B. PCI DSS). Neben dem reinen Inhalt können Sie auch verschieden Ursprung und Entwicklungsprozess aufweisen:

- Internationale, nationale oder europäische Norm mit einem offenen Normungsprozess, z.B. die ISO 27000-Serie
- Privatwirtschaftlicher Standard, z.B. PCI DSS
- Öffentlich-rechtlicher Standard, z.B. BSI Standards

Auch aus rechtlicher Sicht lassen sie sich nach der Verbindlichkeit kategorisieren:

- Verbindliche Standards, deren Einhaltung vom Gesetzgeber vorgeschrieben wird („de jure“)
- Verbindliche Standards, die „de facto“ umzusetzen sind

3.2 ISO 27000-Serie

Die Normenreihe der ISO 27000 befassen sich mit dem Themen der IT- und Informationssicherheit. Diese bestehen unter anderem aus

- einer Norm zum Aufbau eines Informationssicherheitsmanagementsystems (ISO 27001),
- einem Leitfaden für das Informationssicherheits-Management sowie einer Sammlung von Empfehlungen für Anforderungen (ISO 27002),

---

[45] Vgl. [Tipton], Seite 4.
[46] Vgl. [Kersten], Seite 22.

- einer Anleitung zum Umsetzen der ISO 27001 (ISO 27003)
- einer Norm zu Kennzahlensysteme für die Messung der Wirksamkeit eines Informationssicherheitsmanagementsystems (ISO 27004)
- einer Richtlinie für den Aufbau einer Informations- und IT-bezogenen Risikoanalyse (Entwurf ISO 27005).[47]

Die Normen der ISO 27000-Serie bzw. im Allgemeinen der ISO entsprechen der in EU-KOM 315/2011 aufgeführten Normen (Artikel 2 Absatz 1a Verordnung 315/2011).

3.2.1 ISO 27001

Die internationale Norm ISO 27001 beschreibt ein ISMS (Informationssicherheitsmanagementsystem). Kernbestandteil dieses ISMS ist ein kontinuierlicher Prozess zur Verbesserung der Informationssicherheit, der PDCA-Zyklus: Plan – Do – Check – Act. Dieser Zyklus beinhaltet die Planung zur Einführung (Plan), die eigentliche Umsetzung (Do), die Kontrolle der Wirksamkeit der vorherigen Umsetzung (Check) und die eventuell notwendigen Anpassungen oder Verbesserungen (Act). [48] Dieser Prozess beinhaltet in der ersten Phase die Identifizierung und Bewertung von Risiken in der Informationssicherheit.[49] Dieses Risikomanagement ist entscheidend für den Erfolg des ISMS und umfasst folgende Punkte: [50]

- Identifikation von Risiken (Schwachstellen und Bedrohungen)
- Bewertung der Risiken
- Maßnahmen zur Risikobehandlung (Vermeidung, Akzeptanz, Reduktion, Transfer)
- Schriftliche Zustimmung des Managements für verbleibende Restrisiken

Nachdem die ISO 27001 als internationale Norm vom DIN in eine nationale Norm umgesetzt wurde und diese die einzige verfügbare Norm zum Aufbau und Betrieb eines ISMS ist, ist dies Norm für alle Unternehmen defacto verbindlich, die einen ganzheitlichen und risikobasierten Ansatz zur IT-Sicherheit nachweisen müssen.

---

[47] Vgl. [Secorvo], Seite 45f.
[48] Vgl. [Kersten], Seite 40.
[49] Vgl. [Kersten], Seite 44.
[50] Vgl. [Secorvo], Seite 52.

3.2.2 ISO 27002 und ISO 27015

Die Norm ISO 27002 (Code of Practice for Information Security Management) ist ein Leitfaden zur praktischen Umsetzung der Informationssicherheit und beinhaltet eine umfangreiche Sammlung von Empfehlungen.[51] Unternehmen, die ein ISMS nach ISO 27001 betreiben, können in der ISO 27002 eine Auswahl von Maßnahmen finden, um Risiken in der Informationsverarbeitung zu reduzieren. Er beinhaltet 11 Managementgebiete mit insgesamt 133 Maßnahmen.[52] Die noch nicht final veröffentlichte internationale Norm ISO 27015 (Information Security Management Guidelines for Financial Services) erweitert die in ISO 27002 aufgeführten Maßnahmen um Empfehlungen für Unternehmen in der Finanzwirtschaft.

Die Einhaltung der ISO 27002 bzw. später auch die der der ISO 27015 ist nicht verbindlich, da sie nur Empfehlungen ausspricht. Die Empfehlungen sollte aber zumindest beim Aufbau und Betrieb des ISMS nach ISO 27001 beachtet werden.

3.3 Payment Card Data Security Standard (PCI DSS)

Der „Payment Card Data Security Standard“ definiert ein einheitliches Schutzniveau für die Sicherheit von den Karteninhaberdaten einer Kreditkarte. Er stellt in zwölf Kapiteln technische wie organisatorische Anforderungen und soll die allgemeine Sicherheit von Karteninhaberdaten gewährleisten.

3.3.1 Sicherheitsziele

Der PCI DSS besitzt als Sicherheitsziel in der Informationsverarbeitung primär die Vertraulichkeit von Karteninhaberdaten sowie die Nachvollziehbarkeit von Zugriffen auf diese. Die anderen Ziele[53] werden nicht direkt adressiert.[54] Dies drückt sich in den Anforderungskapitel 3 und 4 des Standards aus, die sehr konkrete Anforderungen an die Verschlüsselung dieser Daten beim Transport und bei der persistenten Speicherung stellen. Die weiteren Kapitel 7, 8, 9, 10 und 11 definieren hauptsächlich Zugriffskontrollmaßnahmen sowie die dazugehörige Überwachung. Ergänzt wird dies durch Anforderungen an die Netzwerksicherheit (Kapitel 1 und 2) sowie durch Anforderungen an Anti-Virensoftwaren (Kapitel 5) und an den Softwareentwicklungsprozess (Kapitel 6). Das letzte Kapitel 12 definiert die notwendigen organisatorischen Maßnahmen für die Umsetzung in z.B. Sicherheitsrichtlinien und Standards. Besonders hervorheben muss man die hier aufgeführten Anforderungen 12.1.2

---

[51] Vgl. [Secorvo], Seite 46.
[52] Vgl. [Secorvo], Seite 47.
[53] Kapitel 3.1.
[54] Vgl. [Hauss], Seite 105.

für ein Risikomanagement[55] sowie 12.9.1 an einen Incident Response Plan, der auch Wiederherstellungsstrategien für kritische Infrastrukturen vorsehen soll. Durch diese beiden Anforderungen erweitern sich insbesondere durch das geforderte Risikomanagement die Sicherheitsziele um die allgemeine Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen. Bei Betrachtung der für die beiden Anforderungen vorgeschriebenen Prüfprozeduren stellt sich heraus, dass nur das reine Vorhandensein einer Risikoanalyse bzw. eines jährlichen Prozesses dafür sowie nur ein Incident Response Plan an sich vorhanden sein muss. Besondere qualitative Anforderungen oder Prüfungen werden nicht durchgeführt. Dies steht im Kontrast zu den z.B. sehr konkreten Vorschriften an die Verschlüsselung der Kartennummer, sodass insgesamt die Vertraulichkeit und die Nachvollziehbarkeit von Zugriffen auf diese Daten im Vordergrund stehen.

3.3.2 Organisatrionsstruktur

Der PCI DSS entstammt aus den Bemühungen der einzelnen Kartenunternehmen die Sicherheit ihrer Produkte zu erhöhen und den Missbrauch von Kreditkartendaten zu bekämpfen. Der Vorgänger von PCI DSS ist das „Cardholder Information Security Program“, welches von VISA gegründet wurde und später auch auf eine Kooperation mit MasterCard erweitert wurde. Andere Unternehmen wie zum Beispiel Discover oder American Express hatte jedoch ihre eigenen Programme, sodass Händler mit verschiedenen Sicherheitsanforderungen von verschiedenen Kreditkartenmarken umgehen mussten. Um die Bemühungen der Kartenunternehmen zu vereinheitlichen, schlossen Sie sich zusammen und erstellen den PCI DSS 1.0. Erst danach entstand das Unternehmen, welches für die Weiterentwicklung des Standards verantwortlich ist: Das PCI Security Standards Council. Die Gründungsmitglieder waren American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa International.[56] Somit ist der PCI DSS im Gegensatz zu z.B. ISO 27002 keine internationale Norm, unterliegt auch keinem öffentlichen Normungsverfahren. Zwar ist es für andere Unternehmen durch eine Mitgliedschaft möglich, früher Informationen über Änderungen am Standard zu erhalten, darüber zu diskutieren und auch einen begrenzten beratenden Einfluss aus zu üben, aber die schlussendliche Entscheidungsgewalt über Veränderungen am Standard steht ausschließlich den Gründungsmitgliedern zu. Der Standard selbst

[55] Dort wird verwiesen auf OCTAVE, ISO 27005 und NIST SP 800-30.
[56] Vgl. [Bradley], Seite 20f.

sowie erklärende Unterlagen zu ihm sind im Internet frei zugänglich, sofern die Lizenz akzeptiert wurde[57].

Im Gegensatz zu gesetzlichen Anforderungen wie dem BDSG, ist der PCI DSS kein Gesetz und geht auf die zuvor dargestellte privatwirtschaftliche Initiative zurück. Die Einhaltung des Standards, bzw. der Nachweis der Zertifizierung wird über Verträge zwischen den beteiligten Unternehmen erzwungen. In Anforderungen 12.8 des Standards wird zudem die Überwachung des Compliance-Status von anderen Unternehmen gefordert, sofern für diese auch die Anforderungen des Standards gelten. Dies ist z.B. bei der Weiterleitung von Karteninhaberdaten der Fall, sodass ein Unternehmen keine Karteninhaberdaten an andere Unternehmen weiterleiten darf, sofern diese nicht ein gültiges Zertifikat für die Einhaltung von PCI DSS vorweisen kann. Sollten Anforderungen des PCI DSS nicht eingehalten werden bzw. kann kein gültiges Zertifikat als Nachweis vorgezeigt werden, drohen Vertragsstrafen. Sollten Karteninhaberdaten aus einem Unternehmen unerlaubt kopiert (also ‚gestohlen‘) werden und erfüllte das betroffene Unternehmen zu diesem Zeitpunkt nicht die Anforderungen des PCI DSS, sind weitere Vertragstrafen zu zahlen. Dies ist unabhängig von weiteren Schadensersatzansprüchen, die stellenweise auf $80 pro Karte geschätzt werden.[58]

3.3.3 Zertifizierung

Der Nachweis der Einhaltung des PCI DSS ist u.a. abhängig von den Umsatzahlen eines Unternehmens. Bei geringen Umsätzen reicht das Ausfüllen eines Selbstfragebogens (SAQ). Größere Unternehmen müssen sich von einem durch das PCI Council akkreditierten Prüfer (QSA) zertifizieren lassen.[59] Die ausgestellten Zertifikate besitzen jeweils ein Ablaufdatum und müssen jährlich erneuert werden

3.3.4 Kritische Betrachtung mit europäischem Recht

Der PCI DSS erfüllt nicht die Anforderungen der Verordnung 315/2011 der europäischen Kommission. Um die Anforderungen zu erfüllen, müsste er die in Anhang II aufgeführten Voraussetzungen erfüllen. Dazu müsste der Standard nach Anhang II Abs. 2 von einer gemeinnützigen Organisation entwickelt werden, welche die dort genannten Punkte Offenheit, Konsens und Transparenz erfüllen. Da bereits der erste Punkt der Offenheit nicht erfüllt wird, kann er nicht als technische Spezifikation im Bereich der IKT

---

[57] Siehe auch https://www.pcisecuritystandards.org/.
[58] Vgl. [Bradley], Seite 9 und Seite 26.
[59] Vgl. [Huber], Seite 16f.

angesehen werden. Damit stellt der PCI DSS eine Marktabsprache dar und verursacht durch den Zwang negative Netzwerkeffekte. Somit könnte der vertragliche Zwang zur Erfüllung des PCI DSS ein wettbewerbswidriger Verstoß nach §101 AEUV[60] darstellen.

Auch der Zertifizierungsprozess selbst steht von der Grundstruktur her nicht in Einklang mit europäischem Recht. Die Prüfer werden von einem privaten Unternehmen (PCI Security Standards Council) akkreditiert und nicht von einer nationalen Akkreditierungsstelle. Dies steht in Widerspruch zur Verordnung 765/2008 der Europäischen Kommission, nach der die Akkreditierung eine staatliche Aufgabe ist. Damit sind die Konformitätsbewertungen in Form eines PCI-Zertifikats nicht mit europäischem Recht vereinbar.

[60] Vertrag über die Arbeitsweise der Europäischen Union. Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon

4 Fazit

Kreditinstitute und Finanzdienstleister unterliegen der Aufsicht der BaFin und müssen ein umfassendes Risikomanagement inkl. der Betrachtung der Informationssicherheit nachweisen können.[61] Hierbei sind auch die Anforderungen des BDSG zu berücksichtigen und die Konto- und Abrechnungsdaten in der Risikoanalyse zu integrieren.[62] Um ein Haftungsprivileg zu erzielen, bietet sich eine Zertifizierung nach ISO 27001 an, wobei auf eine Zertifizierung nach BSI-Grundschutz verzichtet werden sollte.[63]

Kreditkartennummern sowie damit verbundene Abrechnungsdaten unterliegen dem Schutz des BDSG.[64] Um hierbei ein Haftungsprivileg zu erreichen, muss ein Informationssicherheitsmanagementsystem nach ISO 27001 betrieben werden. Durch die reine Konformität auf PCI DSS lässt sich kein Haftungsprivileg erreichen, da der Standard keine Norm ist. Direkte Anforderungen für eine aktive Risikovorsorge ergeben sich nach dem KWG nicht.[65] Der PCI DSS umfasst nur die Vertraulichkeit von Karteninhaberdaten (insbesondere der Kreditkartennummer), sodass im Rahmen der Risikoanalyse eines ISMS weitere Maßnahmen zu treffen sind.[66] Des Weiteren kann der vertragliche Zwang PCI DSS zu erfüllen gegen das Wettbewerbsrecht verstoßen und die ausgestellten PCI-Zertifikate nach europäischem Recht ungültig sein.[67]

Unterschrift

Datum: 20. Februar 2012

---

[61] Kapitel 2.2.5.
[62] Kapitel 2.2.6.
[63] Kapitel 2.2.5.
[64] Kapitel 2.1.8.
[65] Kapitel 2.1.6.
[66] Kapitel 3.3.1.
[67] Kapitel 3.3.4.

5 Anhang I. Literaturverzeichnis

[Bradley] Bradley, Tony, et al. PCI Compliance. Burlington: Syngress Publishing Inc., 2007.

[Buck] Buck-Heeb, Petra. Kapitalmarktrecht. 5. Auflage. Heidelberg: C. F. Müller, 2011.

[Chen] Chen, Qingfeng/Zhang, Chengqi/Zhang, Shichao. Secure Transaction Protocol Analysis. Berlin: Springer-Verlag. 2008.

[Einsele] Einsele, Dorothee. Bank- und Kapitalmarktrecht. 2., neu bearbeitete Auflage. Tübingen: Mohr Siebeck.

[Hauss] Hauss, Matthias. Rote Karte. Wie der Sicherheitsstandard der Kreditkartenindustrie beim Datenschutz helfen kann. In: iX. Magazin für professionelle Informationstechnik. Ausgabe 09/2011. Heise-Verlag.

[Huber] Huber, Friedrich et al. Informationssicherheit. Ein Vergleich von Standards und Rahmenwerken. Studie im Auftrag des BSI. Im Internet abrufbar unter https://www.bsi.bund.de/SharedDocs/ Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.pdf?__blob=publicationFile. Abgerufen am 31.01.2012, Stand 2009.

[Kersten] Kersten, Heinrich/Reuter, Jürgen/Schröder, Klaus-Werner. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. 2. Auflage. Wiesbaden: Viewig+Teubner. 2009.

[Kümpel] Kümpel, Siegfried. Wittig, Arne. Bank- und Kapitalmarktrecht. 4. neu bearbeitete Auflage. Köln: Otto Schmidt-Verlag. 2010.

[Nitsch] Nitsch, Karl Wolfhart. Bankrecht für Betriebswirte und Wirtschaftsjuristen. 3. erweiterte Auflage. Bremen: EHV. 2011.

[Spindler-1] Spindler, Gerald. Unternehmensorganisationspflichten. Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte. Universitätsverlag Göttingen. Göttingen. 2011.

[Spindler-2] Spindler, Gerald. Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI. Im Internet abrufbar unter https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30962/Gutachten_pdf.pdf. Abgerufen am 02.02.2012, Stand 2007.

[Secorvo] Secorvo Security Consulting GmbH (Hrsg.). Barzin, Petra u.a. Zentrale Bausteine der Informationssicherheit. Ebersdorf: 1-2-Buch, 2011.

[Tipton] Tipton, Harold F. Official (ISC)² Guide To The CISSP CBK. Boca Raton: Auerbach Publications, 2010.

[Witt] Witt, Bernhard. Datenschutz kompakt und verständlich. 2. Aktualisierte und ergänze Auflage. Wiesbaden: Vieweg+Teubner. 2011.