Eine Welt – ein **Standard**: unterwegs zu mehr **Datensicherheit**

Von Carola Paschola und Kathrin Schier

Mit dem PCI-Standard hat die Kreditkartenindustrie den Schulterschluss für die Sicherheit von sensiblen Kundendaten geschaffen. Dem Einzelhandel lässt sich der Aufwand für die Umsetzung am besten unter Hinweis auf die Vermeidung von Imageschäden und Kosten durch Datenmissbrauch vermitteln, so die Autorinnen. Daneben gibt es auch die Möglichkeit, im PCI Security Standards Council Empfehlungen und Änderungswünsche einzubringen. Dass dies von immer mehr Unternehmen genutzt wird, ist für die Autorinnen ein ermutigendes Zeichen dafür, dass die Verbreitung des Sicherheitsstandards sich beschleunigen wird. Red.

Die Kreditkartenindustrie hat in einem einzigartigen Schulterschluss eine globale Norm für die Sicherheit von sensiblen Kundendaten geschaffen. Ziel des Payment Card Industry Data Security Standard (PCI DSS) ist es, dass sich jede Stelle weltweit, die mit Kreditkartendaten umgeht, diesem Standard anschließt. Anreize gibt es genügend: Der Schutz der sensiblen Kreditkartendaten beugt imageschädigenden Datenskandalen vor und fördert das Vertrauen der Kunden.

Der Schutz sensibler Daten kann in der globalisierten Welt mit ihren weitgehend liberalisierten Märkten und Finanzströmen gar nicht hoch genug angesiedelt werden. Diese Aufgabe lässt sich nur durch ein gemeinsames Engagement aller am bargeldlosen Zahlungsverkehr Beteiligten und mit Hilfe von weltumspannenden Lösungsansätzen bewältigen. Dies haben die führenden Kreditkartenanbieter erkannt und eine Initiative zur Einführung technischer Sicherheitsstandards ins Leben gerufen. Ergebnis ist der gemeinsame Datensicherheitsstandard der Kreditkartenbranche, der „Payment Card Industry Data Security Standard" (PCI DSS).

Branchenübergreifender Ansatz

Bemerkenswert ist dabei zum einen der weltumspannende Ansatz: Die gesamte Kreditkartenbranche steht hinter der Idee und zieht an einem Strang. Zum anderen hatten die Initiatoren von Anfang an die Absicht, die Regeln überall dort zu etablieren, wo Kundendaten gespeichert, übermittelt und verarbeitet werden. Sie betreffen daher sämtliche Vertragspartner mit Kartenterminals, auf Datenspeicherung oder -verarbeitung spezialisierte Dienstleister und viele weitere Unternehmen und Institutionen sowie deren Mitarbeiter, die in irgendeiner Form mit Kreditkartendaten in Berührung kommen.

Der PCI DSS bildet die Basis für die Zusammenarbeit dieses Netzwerks. In seinem branchenübergreifenden Ansatz ist dieser Standard einzigartig.

Ein hohes Maß an Sicherheit im Umgang mit Kreditkartendaten ist im Interesse aller Beteiligten – dies zeigen nicht zuletzt aktuelle Ereignisse, über die die Presse berichtet hat. Jeder Vorfall verdeutlicht, dass es eine 100-prozentige Sicherheit trotz größter Anstrengungen nicht geben kann; der PCI DSS bildet einen Mindeststandard, um das Auftreten von Sicherheitsvorfällen möglichst zu verhindern. Die Ereignisse unterstreichen zudem, dass nichts unversucht bleiben sollte, um alle Möglichkeiten für kriminelle Handlungen im Zusammenhang mit Kundendaten zu vereiteln.

Entscheidend ist, dass die Fälle, in denen Daten in unbefugte Hände gelangen, trotz ihrer medialen Präsenz, eher die Ausnahme denn die Regel sind. Während es weiterhin Einzelhändler und andere Dienstleister gibt, die nicht PCI-konform sind und damit ein höheres Risiko tragen, gibt es

Zu den Autorinnen

Carola Paschola ist Vice President und General Manager, Merchant Services Germany & Austria, **Dr. Kathrin Schier** ist verantwortlich für den Bereich Global Network Operations – Merchant Data Security EMEA bei American Express International Inc., Frankfurt am Main.

eine sehr starke Zunahme an Organisationen, die den PCI DSS anwenden.

Der Standard – von dem Rat erst im vergangenen Jahr eingeführt – wird nun immer häufiger in der Praxis angewandt. Dazu kommen die positiven Auswirkungen, die der neue Standard auf die Strategien und Umsetzungen der Informationssicherheit von Unternehmen in der ganzen Welt hat.

Kreditkarteninhaberdaten müssen in der gesamten Zahlungsbranche – und darüber hinaus – vor Risiken wie finanziellem Betrug wirksam geschützt werden. Das Vertrauen von Kunden in die bargeldlosen Zahlungssysteme muss erhalten und gestärkt werden.

Der Faktor Sicherheit ist nötig, um die Akzeptanz des Kartenwesens bei allen daran angeschlossenen Unternehmen zu erhöhen – und hat damit auch eine nicht zu unterschätzende wirtschaftliche Dimension. Es ist daher von hoher Bedeutung für alle Beteiligten, dass die Initiatoren des PCI DSS bei der flächendeckenden Einführung dieses Standards erfolgreich sind.

Abbildung 1: Die zwölf zentralen Anforderungen des PCI-Datensicherheitsstandards im Überblick

1.	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
2.	Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter
3.	Schutz gespeicherter Karteninhaberdaten
4.	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
5.	Verwendung und regelmäßige Aktualisierung von Antivirensoftware
6.	Entwicklung und Wartung sicherer Systeme und Anwendungen
7.	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf
8.	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
9.	Beschränkung des physischen Zugriffs auf Karteninhaberdaten
10.	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
11.	Regelmäßiges Testen der Sicherheitssysteme und –prozesse
12.	Befolgung einer Informationssicherheits-Richtlinie

Quelle: PCI Security Standards Council

Gemeinsamer Standard als Dach für bestehende Programme

Der Datensicherheitsstandard der Kreditkartenindustrie setzt da an, wo sich mit klaren Regeln eine maximale Wirkung erzielen lässt: an den Systemen, mit denen Kreditkartendaten übermittelt, gespeichert und verarbeitet werden. Der PCI DSS definiert betriebliche und technische Anforderungen für die ordnungsgemäße Speicherung und den Schutz von Daten. Berührt werden hiervon eine Reihe von Systemkomponenten wie etwa Netzwerke, Server, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und eine Reihe weiterer Einrichtungen. Zudem sind zahlreiche Anwendungen, darunter interne und externe (Internet-)Anwendungen, im Katalog des PCI DSS aufgeführt.

Insgesamt zwölf Anforderungen hat die Kreditkartenbranche festgelegt, die von allen Unternehmen, die Kreditkartendaten übermitteln, verarbeiten oder speichern, erfüllt werden müssen. Werden sie den Anforderungen gerecht, gilt der Umgang mit Kreditkartendaten an der betreffenden Stelle als ausreichend gesichert (siehe Abbildung 1). Der PCI DSS verlangt nicht, dass bestimmte Anbieterlösungen eingesetzt werden, was den Unternehmen eine hohe Flexibilität bei der Umsetzung des Standards ermöglicht.

Der PCI DSS ist zwar ein gemeinsamer Standard, der für eine hohe Sicherheit in Unternehmen sorgen kann. Jeder Kreditkartenanbieter hat jedoch seine eigenen Programme, die sicherstellen, dass alle Händler, Dienstleister und Unternehmen, die mit Kreditkartendaten in Berührung kommen, richtlinienkonform sind.

Pflege und Ausbau der eigenen Konformitätsprogramme obliegen jedem einzelnen Unternehmen. Während die gesamte Industrie dem PCI-Standard unterliegt, bestimmen die Konformitätsprogramme, wer welche Prüfdokumente vorlegen muss, welche Klassifizierungsebenen und Gebühren gelten.

Betrachtet man ausschließlich die Kreditkartenunternehmen, so fallen leichte Unterschiede zwischen den Richtlinien der verschiedenen Anbieter auf. Diese ergeben sich aus dem rechtlichen Grundsatz, nach dem in diesem Bereich keine Absprachen getroffen werden dürfen. Jeder Kartenaussteller, darunter American Express, Visa und Mastercard, hat deshalb sein eigenes Richtlinienkonformitätsprogramm, in dem unter anderem festgelegt ist, wie bei Sicherheitsvorfällen vorzugehen ist.

Unterstützung durch die fünf weltweiten Branchenführer

Der bisher zurückgelegte Weg umfasst die Erarbeitung des PCI DSS durch die führenden Kreditkartenunternehmen Mastercard Worldwide, Visa Inc., den japanischen Marktführer JCB International, Discover Financial Services sowie American Express. Im September 2006 wurde die verantwortliche Trägerorganisation „PCI Security Standards Council" gegründet.

Ein besonderes Merkmal der Zusammenarbeit der Initiatoren ist ihre Offenheit für Partner, die sich in der heutigen Struktur des „PCI Security Standards Council",

widerspiegelt. Bereits 500 Unternehmen aus der ganzen Welt und verschiedenen Branchen sind als teilnehmende Organisationen aktiv.

An der Spitze des PCI-Council steht ein Exekutivkomitee, das über Richtlinienkompetenz verfügt und dem hochrangige Vertreter der fünf Gründungsunternehmen angehören. Die operative Entscheidungsbefugnis liegt bei einem Management-Gremium, das sich ebenfalls aus den Kreditkartenanbietern rekrutiert. Der Führungsebene sind Arbeitsgruppen für Marketingfragen sowie für technische und rechtliche Aspekte unterstellt.

Kreditkartenindustrie und Partner optimieren gemeinsam

Um den Interessen aller vom PCI DSS berührten Parteien Raum zu geben, ist ein Beratergremium fest in der Organisation verankert. Hier erhalten Repräsentanten der mittlerweile rund 500 angeschlossenen Institutionen Gelegenheit, aktiv an der Gestaltung des PCI-Standards mitzuwirken.

Aufgabe der teilnehmenden Organisationen ist es, die Rückmeldungen aus aller Welt zu bündeln und in Empfehlungen an die entscheidenden Gremien zu verwandeln – ein gewünschter und sinnvoller Prozess, um den Sicherheitsstandard fortlaufend einem Praxistest zu unterziehen und weiterzuentwickeln.

Im „Council" verläuft die Kommunikation zwischen der Kartenindustrie und ihren Partnern aus unterschiedlichen Bereichen des Kreditkartenwesens wechselseitig – und trägt dadurch entscheidend zur Akzeptanz des PCI DSS bei. Die Teilnehmer können durch ihre Mitarbeit in verschiedenen Arbeitsbereichen die Zukunft des PCI DSS mitbestimmen. Im Gegenzug erhalten sie vorab Entwürfe für Modifikationen oder Neufassungen von Standards und können hierzu Empfehlungen und Änderungswünsche abgeben.

Die Mitgliedschaft steht allen Unternehmen offen, die mit der Zahlungsabwicklung verbunden sind, etwa Hotelketten, Fluggesellschaften, Produzenten von Kartenterminals, Softwareunternehmen und viele mehr. Sichtbares Ergebnis des produktiven Dialogs ist die Version 1.2 des PCI DSS, die es seit Oktober 2008 gibt und viele Anregungen der teilnehmenden Organisationen enthält.

Der „PCI Security Standards Council" stellt allen Unternehmen, die den PCI-Standard einführen, umfangreiche Informationen zur Verfügung[1)].

Ein wichtiges Aufgabengebiet ist auch die Zertifizierung von Sicherheitsdienstleistern weltweit, die den Interessengruppen dabei helfen, die Standards umzusetzen. Listen mit geprüften und zertifizierten Anbietern sind online abrufbar. Mit ihrer Hilfe lassen sich Dienstleister finden, die Rechnernetze regelmäßig einem externen Sicherheitsscan unterziehen, sogenannte Scanvendors oder Approved Scanning Vendors (ASVs). Zudem lassen sich über die Listen Experten ausfindig machen, die bei Begehungen vor Ort prüfen, ob alle Einrichtungen eines Unternehmens dem PCI DSS entsprechen; dies sind Audit-Anbieter oder sogenannte Qualified Security Assessors (QSAs). Alle Bescheinigungen der vom „Council" anerkannten Prüfer werden auch von den fünf großen Kreditkartenanbietern akzeptiert.

Die bisherigen Erfahrungen zeigen, dass die bestehende Infrastruktur gut funktioniert und der PCI DSS sich in der Praxis bereits vielfach bewährt hat. Dennoch befinden wir uns noch in der Phase, in der der Standard nicht überall angewendet wird. Es ist noch ein gutes Stück des Weges zu gehen, bis Kunden sich stets von dieser Norm geschützt wissen, wo immer sie auf der Welt per Kreditkarte zahlen.

Implementierung braucht zwölf bis 18 Monate

Dies ist nicht zuletzt der Tatsache geschuldet, dass seit der Formulierung des Standards nur etwas mehr als zwei Jahre vergangen sind. Außerdem ist die Umstellung auf PCI DSS mit Aufwand auf Seiten der Unternehmen (Händler, Systemanbieter, Dienstleister) verbunden, der erst einmal geleistet werden muss. Dazu gehört auch, alle betroffenen Abteilungen und Mitarbeiter auf die Einführung des Standards vorzubereiten und später die permanente Einhaltung sicherzustellen. Die Erfahrung zeigt, dass bis zum Erreichen

Abbildung 2: Die aktuellen Datenspeicherungsvorschriften nach PCI DSS

	Datenelement	Speicherung zulässig	Schutz erforderlich	Verschlüsselung erforderlich
Karteninhaberdaten	Kreditkartennummer (PAN)	Ja	Ja	Ja
	Gültigkeitsdatum*)	Ja	Ja	Nein
	Servicecode*)	Ja	Ja	Nein
	Name des Karteninhabers*)	Ja	Ja	Nein
Vertrauliche Authentifizierungsdaten**)	Alle Magnetstreifendaten***)	Nein	–	–
	Kartenprüfnummer	Nein	–	–
	PIN	Nein	–	–

*) Diese Datenelemente müssen geschützt werden, wenn sie in Verbindung mit der Kreditkartennummer (PAN) gespeichert werden.
**) Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden (auch wenn sie verschlüsselt wurden).
***) Vollständige Verfolgungsdaten vom Magnetstreifen, Magnetstreifenabbild auf dem Chip oder einem anderen Speicherort.

der PCI-Konformität zwölf bis 18 Monate vergehen können.

Argumente für PCI: Schutz vor Image-Schäden und Kosten bei Missbrauch

Das bei weitem wichtigste Argument für PCI DSS ist der Schutz des Markennamens. Besonders im Online-Handel ist dieser Faktor entscheidend. Wer Missbrauchsmöglichkeiten reduziert, verhindert negative Berichterstattung, die automatisch auf Verstöße folgt. Unternehmen sind auf ein intaktes Vertrauensverhältnis zu ihren Kunden angewiesen. Wenn dieses Vertrauen enttäuscht wird, wirkt sich dies unmittelbar auf die Verkaufszahlen aus. Vertragspartner müssen sich daher fragen, was ihnen ein unbeschädigter Markenname wert ist. Zu welchem Preis könnten sie ihr Produkt verkaufen, wenn ihre Datensicherheit gefährdet war und ihr Markenname gelitten hat? Mit anderen Worten: Welchen Wert hat der Markenname, den PCI DSS zu schützen versucht, für den Kartenakzeptanten?

Ein weiteres Argument, sich dem PCI DSS anzuschließen, betrifft die Absicherung des Vertragsunternehmens im Fall der Fälle. Der Händler oder der Kreditkartenanbieter kann für die Kosten verantwortlich gemacht werden, die durch betrügerische Aktivitäten als Folge eines Sicherheitsvorfalls entstehen. Wenn ein Händler American Express sofort nach Bekanntwerden einer Sicherheitsverletzung informiert, das Unternehmen zum Zeitpunkt des Vorfalls und auch anschließend PCI DSS-konform arbeitete und der Vorfall nicht auf ein Fehlverhalten des Vertragspartners oder einer seiner Mitarbeiter zurückzuführen war, ist der Händler nicht haftbar.

Mit der Anzahl der Transaktionen erhöht sich die Nachweispflicht

Aufgrund seiner universellen Anwendbarkeit ist der PCI-Standard eine geeignete Ausgangsbasis, auf der sich Unternehmen länder- und branchenübergreifend auf ein gemeinsames Verständnis von Datensicherheit festlegen können. Für die Implementierung gelten klare Regeln ebenso für zu erbringende Nachweise, dass der Standard eingehalten wird: Je mehr Transaktionen ein Partner aufweist, desto höher sind die Anforderungen, die PCI-Konformität nachzuweisen.

Auf der Ebene 1 eingestufte, aktive Vertragspartner müssen eine jährliche Prüfung durch einen zertifizierten QSA nachweisen, auf deren Basis ein Audit/Konformitätsbericht/Report on Compliance erstellt wird. Die Prüfung muss für alle Systemkomponenten durchgeführt werden, die zur Verarbeitung, Speicherung oder Übertragung von Karteninhaberdaten genutzt werden. Ebenfalls Pflicht sind vierteljährliche Netzwerk-Scans. Bei diesem Verfahren werden die an das Internet angeschlossenen Computernetzwerke und Webserver des Vertragspartners per Fernzugriff geprüft, um sicherzustellen, dass keine Sicherheitslücken bestehen. Durch die Scans werden die Systeme auf potenzielle Schwächen und Anfälligkeiten hin getestet.

Die Konformität wird nur anerkannt, wenn keine gravierenden Sicherheitsmängel vorliegen. Wenn der Vertragspartner das Verfahren für die Richtlinienkonformität eingeleitet hat, akzeptiert American Express einen Projektplan mit den Einzelheiten der erforderlichen Aufgaben und mit einem angemessenen Zeitrahmen bis zur vollständigen PCI DSS-Konformität.

Das Vorgehen der Kreditkartenunternehmen unterscheidet sich auch in der Begleitung der Vertragsunternehmen bei der Einführung des PCI DSS. American Express richtet sich mit einem kostenlosen Angebot an Vertragspartner. Diese können verschiedene Serviceleistungen in Anspruch nehmen, die sie bei der Umsetzung der PCI-Konformität unterstützen.

Die zügige und umfassende Verbreitung des PCI-Datensicherheitsstandards ist im Interesse aller Beteiligten, einschließlich der Endverbraucher, die von mehr Sicherheit profitieren. Es ist daher davon auszugehen, dass sich die bereits begonnene Entwicklung nach den positiven Erfahrungen in den ersten zwei Jahren fortsetzen und deutlich beschleunigen wird.

Ermutigend ist insbesondere, dass bereits zahlreiche Unternehmen die Mitsprachemöglichkeiten des „PCI Security Standards Council" wahrnehmen. Eine Idee aus dem Handel ist die Einführung eines Gütesiegels, das Verbrauchern die Anwendung des PCI DSS signalisiert. Die Chancen stehen gut, dass bezüglich der Sicherheit große Fortschritte unternommen werden – auch wenn noch viel zu tun bleibt.

Vertragspartner-Service bei Einführung von PCI

Die Kreditkartenanbieter gehen unterschiedliche Wege, um ihre Partner in Handel, Gewerbe und Tourismus bei der Einführung des PCI-Datensicherheitsstandards zu begleiten. Um den Weg zur PCI-Konformität für Partner möglichst einfach zu gestalten, bietet American Express in Kooperation mit dem Sicherheitsunternehmen Trustwave kostenlos Unterstützung an.

In bestimmten Märkten steht allen Vertragspartnern der Ebene 1 und 2 – also mit mehr als 50 000 Kreditkarten-Transaktionen jährlich – eine kostenfreie technische Hotline für Fragen rund um PCI DSS sowie das spezifische Datensicherheitsprogramm von American Express (DSOP) zur Verfügung. Ein weiteres Service-Angebot ist darüber hinaus die kostenlose Durchführung der vierteljährlichen Scans der Rechnernetze in den Partnerfirmen für bis zu zehn öffentliche IP-Adressen in den ersten zwölf Monaten.

Fußnote:

[1] Unter der Internetadresse www.pcisecuritystandards.org sind unter anderem Details zum Standard, Listen mit Sicherheitsgutachtern und Prüfungsunternehmen sowie Möglichkeiten zur Mitarbeit in den Gremien zu finden.