Bankmanagement-**Glossar**

Was ist PCI?

Von Ewald Judt und Claudia Klausegger

Ausgelöst durch die steigende Anzahl von Kartentransaktionen und die Gefahren, denen Kartendaten und Kartentransaktionen ausgesetzt sind, beschlossen die Kartenorganisationen American Express, Discover Financial Services, JCB, Mastercard Worldwide und Visa International eine abgestimmte Vorgehensweise. Sie gründeten die PCI Security Standards Council, LLC in Delaware, USA, und luden alle interessierten Parteien ein, ebenfalls Gesellschafter zu werden.

In der Organisation wurde der Payment Card Industry Data Security Standard, meist abgekürzt als PCI oder gelegentlich auch als PCI DSS, erarbeitet. Das Regelwerk für den Kartenzahlungsverkehr bezieht sich auf die Sicherheit von Kartendaten und die sichere Abwicklung von Kartentransaktionen. Mit PCI werden zwei Bereiche abgedeckt. Zum einen enthält das Regelwerk eine Fülle von Anforderungen für das technische Equipment, um Kartendaten sicher zu speichern, zu verarbeiten und zu übertragen. Zum anderen schreibt PCI für alle Beteiligten periodische Tests vor: Diese reichen von „self-assessments" über einen „security scan" bis zum „security audit". Die Anforderungen des PCI Security Standards Council sind wie folgt strukturiert:

Errichtung und Wartung eines sicheren Netzwerks: 1. Installation und Erhaltung einer Firewall-Konfiguration zum Schutz der Daten der Karteninhaber. 2. Keine Verwendung von Standardvorgaben des Lieferanten für System-Passwörter oder sonstige Sicherheitsparameter.

Schutz der Karteninhaberdaten: 3. Schutz der gespeicherten Karteninhaberdaten. 4. Verschlüsselte Übertragung der Karteninhaberdaten über offene, öffentliche Netzwerke.

Aufrechterhaltung eines Schwachstellen-Managementprogramms: 5. Verwendung und regelmäßige Aktualisierung von Anti-Virus-Software. 6. Entwicklung und Wartung sicherer Systeme und Anwendungen.

Einführung wirksamer Zugangsmaßnahmen: 7: Beschränkung des Zugangs zu Karteninhaberdaten auf geschäftliche Notwendigkeiten. 8. Vergabe einer einmaligen ID an jede Person mit Computerzugang. 9. Beschränkung des physischen Zugangs zu den Karteninhaberdaten.

Regelmäßige Überwachung und Prüfung der Netzwerke: 10. Verfolgung und Überwachung aller Zugriffe auf Netzwerkressourcen und Karteninhaberdaten. 11. Regelmäßige Tests der Sicherheitssysteme und -verfahren.

Einhaltung von Informationssicherheitsregeln: 12: Einhaltung von Regeln, die die Informationssicherheit gewährleisten.

Am einfachsten ist dabei das „self-assessment", bei dem der Kartenakzeptant oder der Service Provider einen Bogen mit 74 Fragen ausfüllen muss. Beim „security scan" werden Kartenakzeptanten und Serviceprovider von einem ASV, einem „approved scanning vendor", geprüft. Dieses Scanning wird via Internet durchgeführt und soll die Sicherheit der Architektur und der Konfiguration des Systems checken. Das „security audit" wird von einem QSA, einem „qualified security assessor", durchgeführt. Es beinhaltet die Überprüfung der Dokumentation von Sicherheitsmaßnahmen auf Vollständigkeit und Zweckmäßigkeit sowie eine Inspektion vor Ort, bei der die Übereinstimmung aller Systeme und Applikationen mit dem PCI DSS validiert wird.

Die Art, wie die Einhaltung der PCI-Vorschriften überprüft werden, ist primär abhängig von der Anzahl der Kartentransaktionen, die ein Kartenakzeptant (Merchant) oder ein Dienstleister (Serviceprovider) abwickelt.

Level 1: Bei Händlern oder Dienstleistern, wo Kartendaten bereits komprimittiert wurden, sowie solchen, die mehr als sechs Millionen Kartentransaktionen pro Jahr abwickeln, findet vierteljährlich ein PCI Network Scan und jährlich ein PCI Audit statt.

Level 2: Bei Händlern oder Dienstleistern, die zwischen einer Million und sechs Millionen Kartentransaktionen abwickeln, findet vierteljährlich ein PCI Network Scan statt und ist jährlich ein PCI Self-Assessment erforderlich.

Level 3: Bei Händlern oder Dienstleistern, die zwischen 20 000 und einer Million E-Commerce-Kartentransaktionen abwickeln, findet vierteljährlich ein PCI Network Scan statt und ist jährlich ein PCI Self-Assessment erforderlich.

Level 4: Bei allen anderen Händlern oder Dienstleistern findet jährlich ein PCI Network Scan statt und ist jährlich ein PCI Self-Assessment erforderlich.

Dr. Ewald Judt ist Honorarprofessor der Wirtschaftsuniversität Wien und Geschäftsführer der PayLife Bank GmbH; ewald.judt@paylife.at/www.paylife.at. Dr. Claudia Klausegger ist Assistenzprofessorin am Institut für Marketing-Management der Wirtschaftsuniversität Wien; claudia.klausegger@wu-wien.ac.at.