Kreditkartenindustrie verlangt Sicherheitsmaßnahmen

Schutzzwang

Randolf Skerka, Manuel Atug

Seit Langem schon doktert die Kreditwirtschaft an verbindlichen Sicherheitsmaßnahmen für Unternehmen, die Kartendaten von Zahlungssystemen verarbeiten, herum. Jetzt ist Schluss mit lustig: Vehement fordern Kreditkartenanbieter die Umsetzung des Standards PCI DSS und verhängen immer häufiger Strafen bei Unterlassung.

Liest man die Schlagzeilen eines IT-Newstickers, muten die Meldungen an wie aus einem Cyberkrimi: Dem US-Einzelhändler TJX werden, wie die Öffentlichkeit im März 2007 erfährt, über einen Zeitraum von anderthalb Jahren über 90 Millionen Kreditkartendaten gestohlen, die Bilanz des börsennotierten Unternehmens weist hierfür im ersten Quartal 2008 250 Mio. US-$ Rückstellungen aus. Im April 2007 wird der Server des Softwareherstellers Valve kompromittiert und mehrere Tausend Kreditkartennummern geraten in die Hände der Eindringlinge. In Deutschland waren im Oktober 2007 über 60 000 Kunden des Online-Tickethändlers Kartenhaus vom Kreditkartendatendiebstahl betroffen. Und schließlich wird selbst das britische Militär im Januar 2008 Opfer eines Diebstahls privater Informationen mehrerer Hunderttausend Rekruten.

Für den Handel mit gestohlenen Kreditkartendaten hat sich mittlerweile ein reger Schwarzmarkt entwickelt. Nach Informationen des LKA Baden-Württemberg erzielen die Daten einer einzelnen Kreditkarte Preise zwischen 50 und 150 Euro. Für die Betroffenen ist der Schaden ungleich höher. Man kann davon ausgehen, dass pro missbräuchlich genutzter Kreditkarte ein durchschnittlicher Schaden von zwei- bis dreitausend Euro entsteht, bevor die Bank die Karte sperrt.

Direkte und indirekte Schäden

Dementsprechend hoch sind die Schadenersatzanforderungen, denen sich ein Unternehmen im Schadensfall gegenüber sieht. Bei nur 3000 Kreditkartentransaktionen im Monat sammelt sich während der üblichen Gültigkeitsdauer von drei Jahren ein Datenschatz von 120 000 Kreditkartensätzen an. Damit beträgt allein der durch den Missbrauch der Karten direkt entstandene Schaden geschätzte 240 Millionen Euro. Dabei sind die Kosten für neu zu emittierende Kreditkarten, Rechtsstreitigkeiten und den gravierenden Imageschäden noch nicht berücksichtigt.

Der Schutz von Karteninformationen ist für jedes Unternehmen deshalb schon aus Eigeninteresse von höchster Priorität. Zusätzlich verlangen die Anbieter internationaler Zahlungssysteme – darunter MasterCard und Visa – die Umsetzung des Payment Card Industry Data Security Standard (PCI DSS) von allen Unternehmen, die Kartendaten der internationalen Zahlungssysteme verarbeiten, speichern oder weiterleiten. Dies sind unter anderem E-Commerce-, sogenannte MoTo- (Mail order/Telephone order) und „klassische“ POS-Händler (Point of Sale) sowie deren Service Provider, etwa Webhoster, Payment Service Provider, Rechenzentrumsbetreiber, Fraud-Management-Dienstleister, Acquirer, Issuer und Prozessoren.

Die Einhaltung des Standards ist für alle verbindlich, ob großer oder kleiner Händler oder Service Provider. Aller-

iX-TRACT

- Wer Kartendaten der internationalen Zahlungssysteme Visa & Co. verarbeitet, speichert oder weiterleitet, ist zur Einhaltung des Sicherheitsstandards PCI DSS verpflichtet.
- Die Nachweise für die Umsetzung – externe Audits oder Selbsterklärung – hängen vom Transaktionsvolumen ab. Service Provider etwa müssen zwingend akkredierte Auditoren beauftragen.
- Wer den Standard nicht einhält, muss im Schadensfall mit erheblichen Vertragsstrafen und Schadensersatzforderungen rechnen.

dings unterscheidet der Standard die Zertifizierung, die sogenannte Compliance Validation, nach verschiedenen Händler- und Service-Provider-Abstufungen (Level). Nur Händler Level 1 (mehr als 6 Mio. Kartentransaktionen im Jahr von MasterCard oder Visa, oder mehr als 2,5 Mio Kartentransaktionen im Jahr von Amex) und Service Provider müssen die Einhaltung durch ein PCI DSS Security Audit und vier PCI DSS Security Scans im Jahr nachweisen. Bei kleineren Händlern reichen als Nachweis die Beantwortung eines PCI DSS Self-Assessment Questionnaire sowie die Durchführung von vier PCI DSS Security Scans im Jahr.

Unterschiedliche Fristen je Anbieter

Große Level-1-Händler dürfen wahlweise das PCI DSS Security Audit intern durchführen, Service Provider müssen allerdings immer einen akkreditierten Auditor damit beauftragen. Security Scans dürfen ausschließlich akkreditierte Scan-Dienstleister durchführen.

Die Fristen, bis wann die Einhaltung durch erfolgreiche Zertifizierung nachzuweisen ist, geben die Zahlungssystemeanbieter im Rahmen ihrer PCI-DSS-Compliance-Programme unterschiedlich vor. Die Programme sind im Einzelnen:
– American Express: Data Security Operating Policy (DSOP)
– Discover: Discover Information Security Compliance (DISC)
– JCB: Data Security Program
– MasterCard: Site Data Protection (SDP)
– Visa USA: Cardholder Information Security Program (CISP)
– Alle anderen Visa-Regionen: Account Information Security (AIS)
Einige Fristen sind bereits verstrichen, andere laufen bald aus. Der Nachweis bei allen Service-Providern nach Visa AIS beispielsweise war bis spätestens 30. Juni 2005 zu erbringen. MasterCard SDP schreibt ebenfalls vor, dass Händler Level 1 und 3 (die Level definieren sich je nach Anzahl der Transaktionen pro Jahr) bis spätestens 30. Juni 2005 den Nachweis erbringen mussten, Händler Level 2 erhielten von MasterCard aufgrund einer Anpassung der Leveldefinition Aufschub bis 31. Dezember 2008.

Darüber hinaus gibt es immer wieder Ergänzungen und Präzisierungen, die zum Teil einen eigenen Stichtag haben – etwa die jüngste Erweiterung des PCI DSS im Bereich „Entwicklung und Wartung sicherer Systeme und Anwendungen“ (Requirement 6.6): Die auf Webapplikationen gemünzte Anforderung schreibt vor, diese vor bekannten Angriffen zu schützen – sei es durch Codereviews oder spezielle Web Application Firewalls. Zum 30. Juni 2008 wird aus dieser bislang empfohlenen Best-Practice-Maßnahme verbindliche Pflicht. Fachleuten zufolge ist das im April hierzu veröffentlichte Dokument „Information Supplement: Requirement 6.6 – Code Reviews and Application Firewalls Clarified“ auf den Webseiten des PCI SSC allerdings entgegen der eigentlichen Intention wenig präzise und teilweise missverständlich verfasst.

Schon 2000 beziehungsweise 2001 haben MasterCard und Visa angesichts der steigenden Missbrauchsraten im Umfeld von Kartentransaktionen die Programme MasterCard SDP und Visa AIS ins Leben gerufen, um die Sicherheit von Kartendaten bei der Verarbeitung, Speicherung und Weiterleitung zu gewährleisten.

Ende 2004 (MasterCard) bis Anfang 2005 (Visa) haben die Verantwortlichen die bis zu diesem Zeitpunkt voneinander unabhängigen technischen Anforderungen in den PCI DSS zusammengeführt, den der Payment Card Industry Security Standards Council (PCI SSC, www.pcisecuritystandards.org) seitdem weiterentwickelt. Neben MasterCard Worldwide und Visa Inc sind American Express, Discover Financial Services und JCB International weitere Gründungsmitglieder.

Im September 2006 wurde der Standard selbst und im Februar 2008 auch der Selbstbewertungsfragebogen (Self-Assessment Questionnaire) überarbeitet. Der PCI DSS setzt sich derzeit zusammen aus dem eigentlichen Standard, dem Fragebogen, Sicherheitsscans und -audits sowie neuerdings einer Softwarevalidierung:
– PCI Data Security Standard, Version 1.1
– PCI DSS Self-Assessment Questionnaire, Version 1.1
– PCI DSS Security Scanning Procedures, Version 1.1
– PCI DSS Security Audit Procedures, Version 1.1
– PCI Payment Application Data Security Standard, Version 1.1

Vereinfachungen für Anwender

Im April 2008 wurde das von Visa vormals als Visa Payment Application Best Practices veröffentlichte Softwareprüfverfahren unter dem Namen PCI Payment Application Data Security Standard (PA-DSS) eingegliedert. Dieser stellt eine Ableitung eines „Software-Standards“ aus dem PCI Data Security Standard dar, dessen Ziel es ist, den Anwender durch Einsatz der Software beim Einhalten des PCI DSS zu unterstützen.

Das PABP-Zertifizierungsschema läuft zum Ende September aus. Ab Oktober ist Software daher ausschließlich nach dem neuen PA-DSS zu prüfen. Neu im PA-DSS ist, dass im Standard und den begleitenden Dokumenten darauf hingewiesen wird, dass eine Überarbeitung durch das PCI SSC im Zweijahreszyklus erfolgen wird, was sowohl die Planungs- und Investitionssicherheit als auch Release-Wechsel und darauf resultierende Migrationsplanungen bei Softwareherstellern, Integratoren und Kunden erleichtert. Gleiches ist zukünftig auch für den PCI DSS angekündigt.

Da der PA-DSS von Visa in den USA bereits in fünf vorgeschriebenen Schritten bis zum Jahr 2010 verpflichtend wird, ist auch in Europa die Verpflichtung zur ausschließlichen Nutzung von zertifizierter Payment-Software in naher Zukunft zu erwarten.

Für Oktober 2008 hat der PCI SSC eine überarbeitete Fassung des PCI DSS angekündigt. Council-Mitglieder und akkreditierte Partner erhalten einen Entwurf der neuen Fassung zur Kommentierung circa 45 Tage vorab.

Zusätzlich zu den frei verfügbaren Standards hält die Webseite des PCI SSC weiteres Material bereit, etwa den PCI DSS in verschiedenen weiteren Sprachen – zum Beispiel Deutsch, Französisch und Spanisch –, aber auch Interpretationsunterstützungen wie das Dokument „Navigating PCI DSS – Understanding the Intent of the Requirements“ sowie ein Glossar.

Wer im Falle der Kompromittierung von Kartendaten nicht nachweisen kann, den Anforderungen dieses Standards genügt zu haben, riskiert empfindliche Vertragsstrafen und Schadensersatzanforderungen. Im Gegenzug gewähren die Kreditkartengesellschaften eine teilweise oder vollständige Befreiung von

Organisatorische Kernpunkte

– geregeltes Change-Management
– anerkanntes Key-Management
– sorgfältige Systemdokumentation
– Genehmigungsprozesse
– Sicherheitskonzepte

den vertraglichen Strafzahlungen („Safe Harbor Rule“), wenn sie den Standard zum Zeitpunkt der Kompromittierung als voll erfüllt ansehen und eine Zertifizierung durchgeführt wurde.

Allgemein gesprochen befasst sich der PCI DSS mit dem Schutz von Kreditkartendaten. Dafür bedient er sich zwölf übergeordneter Anforderungen („Requirements“; siehe Kasten „Die zwölf Anforderungen …“), die sich jeweils einem spezifischen Aspekt der Sicherheit von Kartendaten widmen. Jedes übergeordnete Requirement enthält eine Reihe konkreter Handlungsanweisungen, die für eine Zertifizierung ausnahmslos zu erfüllen sind. Dabei sind technische Sicherheitsanforderungen auf Netzwerk-, System- oder Applikationsebene ebenso enthalten wie organisatorische und personelle Maßnahmen zum Erreichen sicherer Geschäftsprozesse im Umgang mit Kartendaten (siehe Kasten „Organisatorische Kernpunkte“).

Technischer Schutz allein genügt nicht

Damit wollen die Verantwortlichen dem Umstand Rechnung tragen, dass eine ausschließlich technische Lösung heutzutage keine ausreichende Sicherheit mehr bieten kann. Selbst bei Einsatz der besten Firewalls ist jedes System im Zweifelsfalle nur so sicher wie das schwächste Passwort, das seine Nutzer verwenden. Auf den ersten Blick mag dies übertrieben klingen, doch mithilfe von im Internet frei verfügbaren Hackingtools lassen sich kleinste Schwachstellen wie ein nachlässig gewähltes Passwort oder ein fehlendes Sicherheits-Update auch durch relativ ungeübte Hacker leicht und schnell ausnutzen, um Zugriff auf ein ansonsten sicheres System zu erlangen.

Deshalb setzt der PCI DSS auf eine tiefgreifende Verwurzelung der Sicherheitsmaßnahmen in den Systemen selbst: Diese sind so zu konfigurieren, dass beispielsweise das Wählen unsicherer Passwörter grundsätzlich ausgeschlossen wird. Daneben ergeben sich durch eine PCI DSS-Zertifizierung tiefschürfende Änderungen in einer ganzen Reihe unterschiedlichster Unternehmensprozesse, von denen sich viele nicht auf die IT-Abteilung beschränken lassen.

So fordert der Standard unter anderem einen hinreichenden Zugriffsschutz von Kartendaten, was neben der möglichst restriktiven Verteilung von Zugriffsrechten in Computersystemen auch die Einführung von offen zu tragenden Mitarbeiterausweisen oder die Installation von Videokameras und Zugangskontrollen mit sich bringt.

Auswirkungen im Tagesgeschäft

Obgleich sich ein Großteil der Änderungen für die meisten Nutzer weitgehend unbemerkt in die Sicherheitsarchitektur der IT-Landschaft integrieren wird, haben einzelne Anforderungen des PCI DSS spürbare Auswirkungen auf das Arbeiten im Tagesgeschäft. Nicht alle dieser Änderungen werden das Arbeiten erleichtern, einige betreffen liebgewonnene Abläufe. Doch alle vom PCI DSS geforderten Maßnahmen sind notwendig, um den Schutz der Kartendaten sicherzustellen und den Fortbestand und das Vertrauen in die Zahlungssysteme zu gewährleisten.

Die Zahlungssystemanbieter teilen Händler und Service Provider nach Transaktionsvolumen oder Art der Dienstleistung in unterschiedliche Level ein. Die Händlerklassifizierung von MasterCard und Visa sowie die Service-Provider-Klassifizierung der beiden sind im Detail verfügbar (siehe *iX*-Link), weniger ausführliche Informationen gibt es auch bei anderen Zahlungssystemen. Händler können das PCI DSS Security Audit intern durchführen.

Die Bewertung (Compliance Validation) von PCI DSS Security Scans sowie bei Service-Providern durchzuführenden PCI DSS Security Audits erfolgt ausschließlich durch akkreditierte Partner (PCI Approved Scanning Vendor beziehungsweise PCI Qualified Security Assessor) des PCI Security Standards Council.

Weder Händler noch Service Provider werden sich dem PCI DSS langfristig entziehen können. Insbesondere MasterCard und Visa, aber neuerdings auch American Express fordern den Nachweis zur Einhaltung des PCI DSS immer vehementer ein. Auch sprechen die Anbieter inzwischen immer häufiger Vertragsstrafen in Form von Penalen zur Nichteinhaltung des PCI DSS aus.

Der Payment Card Industry Security Standards Council hat den PCI DSS über die Jahre mehrfach überarbeitet. Entstanden ist ein ganzes Framework, das wohl auch zukünftig an neue Bedrohungen und Risiken angepasst werden wird – wie kürzlich durch die Einführung des Payment Application Data Security Standard (PA DSS) geschehen. Neben bereits etablierten Sicherheitsstandards wird sich der PCI DSS langfristig einen Platz sichern. (ur)

RANDOLF SKERKA UND MANUEL ATUG

sind Berater bei SRC Security Research Consulting in Bonn.

iX-Link ix0807124

Die zwölf Anforderungen des PCI DSS

1. Einrichtung und Unterhaltung eines sicheren Netzwerks

Anforderung 1: Installation und Verwaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Anforderung 2: Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter

2. Schutz von Karteninhaberdaten

Anforderung 3: Schutz von gespeicherten Karteninhaberdaten

Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke

3. Verwalten eines Programms zur Bewältigung von Sicherheitsrisiken

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen

Anforderung 6: Entwicklung und Verwaltung sicherer Systeme und Anwendungen

4. Implementieren strikter Zugriffssteuerungsmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten auf die geschäftlich erforderlichen Daten

Anforderung 8: Zuweisung einer eindeutigen ID zu jeder Person mit Computerzugriff

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

Anforderung 10: Protokollieren und Prüfen aller Zugriffe auf Daten von Kreditkarteninhabern

5. Regelmäßiges Überwachen und Testen von Netzwerken

Anforderung 11: Regelmäßiger Test von Sicherheitssystemen und -prozessen

6. Verwalten einer Informationssicherheitsrichtlinie

Anforderung 12: Verwaltung einer Informationssicherheitsrichtlinie für Mitarbeiter und beauftragte Unternehmen