



Zertifikat gegen den Datenklau

VISA und Mastercard erhöhen durch neue Strategien die Sicherheit für Kreditkartenkunden im Onlinehandel. Zertifizierungspartner helfen bei der reibungslosen Implementierung.

(erschienen in E-Commerce Magazin 02/2006, S. 50f; Autor: Thomas Schumacher)

Alle Jahre wieder sorgt der Onlinehandel für neue Umsatzrekorde im Weihnachtsgeschäft. Internet-Shopping liegt im Trend, der Einkauf jenseits der traditionellen Ladenöffnungszeiten boomt. Mehr und mehr kommen dabei auch mobile Endgeräte wie PDAs oder Smartphones zum Einsatz, die den digitalen Einkauf auch von unterwegs aus möglich machen. Neben „realen“ Waren werden zunehmend auch digitale Inhalte nachgefragt, etwa Musikstücke, Spiele oder Videoclips. Neuralgischer Punkt bei allen Online-Transaktionen, insbesondere bei mobilen, ist aber immer noch die sichere Bezahlung. Nach dem Scheitern verschiedener digitaler Zahlungsmethoden steht heute unter den angebotenen Zahlungsmöglichkeiten die Kreditkarte an führender Position. „Zahlreichen Kaufwilligen ist die Eingabe der Kreditkartendaten online jedoch zu riskant - und das nicht zu Unrecht, denn leider nimmt mit steigenden Internetumsätzen auch die Kreditkartenkriminalität zu“, so Thorsten Schröter, Solution Unit Manager Security beim Schweizer Systemhaus Trivadis, das als einer von derzeit zwei Zertifizierungspartnern in Deutschland sowohl von MasterCard als auch von VISA akkreditiert ist. Weil dadurch große Schäden entstehen und das

Vertrauen aller Abwicklungspartner vom Anbieter bis zum Kunden leidet, sind neue Sicherheitsvorkehrungen gefordert. VISA und MasterCard haben entsprechende Sicherheitsstandards und Zertifizierungsvorgehen definiert, die in Zukunft als Voraussetzung für eine Zahlungsabwicklung dienen sollen. Payment-Serviceprovider und Onlineshops, die diese zusätzliche Sicherheit heute bereits implementieren wollen, können dazu auf qualifizierte Zertifizierungspartner zurückgreifen.

Schäden in Milliardenhöhe

Der Betrug mit Kreditkartendaten entwickelt immer neue Formen. Waren es früher vereinzelte „Einbrüche“, um Kundeninformationen auszulesen, so reicht das Problem heute bis hin zum Diebstahl ganzer Datenbanken und Identitäten. Dies ist nicht nur für die bestohlenen Kartenbesitzer ein Problem, sondern immer mehr auch für Shopbetreiber. Eine sichere Kreditkartentransaktion setzt immer voraus, dass der Merchant seriös agiert und auf der anderen Seite der Kunde auch tatsächlich der legitime Besitzer der Karte ist. Die Attacken erstrecken sich auf die ganze Kette der Beteiligten im Zahlungsablauf, also vom Merchant über die Abrechnungspartner bis

zu den Käufern. Besonders gefährdet sind dabei die Punkte, an denen große Mengen an Daten aufbewahrt und verwaltet werden. Der Diebstahl ganzer Kundendatenbanken – wie jüngst in den Vereinigten Staaten von Amerika geschehen - stellt dabei den schlimmstmöglichen Fall für alle Beteiligten, einschließlich der Karten ausgebenden Institute selbst, dar. Im Juni dieses Jahres sind Hacker beim US-amerikanischen Dienstleister CardSystem Solutions eingedrungen und haben dabei rund 200.000 Datensätze entwendet. Selbst in Deutschland haben Banken daraufhin Karten ihrer Kunden austauschen müssen. Die in den letzten Jahren erfassten Schäden durch Kreditkartenbetrug gehen in die Milliarden. Allein im Jahr 2003 nahmen die Fälle nach einer Studie von Celent Communications um fast 60 % zu. Mittlerweile liegt die Internetkriminalität im Verhältnis zum „traditionellen“ Kreditkartenmissbrauch um das Zwanzigfache höher und erreicht 2,1 % des Transaktionsvolumens. Und dies ist nur die Spitze des Eisbergs, denn Fälle dieser Größenordnung werden nur selten bekannt. Experten gehen von einer erheblichen Dunkelziffer von Missbrauchsfällen aus, die nicht an die Öffentlichkeit geraten.

Sicherheit nach gemeinsamem Standard

Für die Kartenanbieter sind dies alarmierende Zahlen, auf die eine Reaktion erfolgen musste. VISA und MasterCard haben daher Sicherheitsprogramme ins Leben gerufen, welche die Sicherheit bei Kreditkartenzahlungen sowohl für den Kunden als auch für alle beteiligten Partner innerhalb der Kette der Zahlungsabwicklung erhöhen. Dies geschieht auf zwei Ebenen: Unter den Begriffen „Verified by VISA“ und „MasterCard SecureCode“ wird zuerst der Informationsaustausch zwischen Kunde und Onlineshop sicherer gestaltet, indem neben Verschlüsselung und der direkten Verbindung mit einer zentralen Abrechnungsstelle die Eingabe einer PIN erforderlich ist. Auf Seiten des Kunden ist dazu lediglich ein internet- und browserfähiges Endgerät erforderlich, das die vorgeschriebenen Mindeststandards für eine verschlüsselte Datenübertragung unterstützt. Heute gilt dies bereits für nahezu alle PDAs sowie zahlreiche Smartphones und Handys. Für Shopbetreiber wird das Risiko minimiert, Waren gegen Kreditkartenbezahlung anzubieten, da sie dadurch die Gewähr haben, mit dem wirklichen Besitzer der Karte zu kommunizieren.

VISA und MasterCard haben schon vor einigen Jahren mit ihren jeweils eigenen Programmen begonnen. Beide Kartenanbieter haben erkannt, dass sie in ihren Sicherheitsbestrebungen die gleichen Ziele verfolgen und dass sich die erarbeiteten Sicherheitsstandards sehr ähnlich sind. Sowohl das Account Information

Security Program (AIS) von VISA als auch das Pendant von MasterCard, die Site Data Protection (SDP), definieren international gültige Vorschriften über die Verwendung, den Schutz, die Benutzung, Speicherung und Bereitstellung von Konto- und Transaktionsdaten. Als zweite Sicherheitsebene entstanden daraus die Payment Card Industry (PCI) Requirements, die Anfang 2005 in Kraft getreten sind. Diese sehen für alle Unternehmen, die Karten- oder Transaktionsdaten speichern, die Durchführung eines Audits vor. Dabei wird für jedes Unternehmen die Gefährdung je nach Transaktionsvolumen, Umsatz und Funktion (z.B. Onlineshop, Payment Service Provider, Hoster) unterschiedlich bewertet. Entsprechend sind auch die Anforderungen zur Überprüfung, je nach Risikogruppe ist ein Self-Assessment-Fragebogen auszufüllen, eine Fernüberprüfung (Security Scan) zu bestehen oder zusätzlich auch eine Vor-Ort-Überprüfung (Onsite Review) erforderlich. Nach erfolgreich bestandener Überprüfung ihrer organisatorischen und technischen Sicherheitsmassnahmen durch einen akkreditierten Sicherheitspartner erhalten die Prüflinge schließlich ihr Zertifikat. Trivadis hat bereits zahlreiche Kunden durch den gesamten Prozess der Zertifizierung begleitet, darunter die Payment-Serviceprovider Saferpay und Datatrans. Die organisatorische Überprüfung umfasst Sicherheitsaspekte wie die Existenz einer Security-Policy, die den Vorgaben von VISA und MasterCard entspricht, das Sicherheitsdispositiv und die Verantwortlichkeiten, implementierte Si-

cherheitslösungen und Prozesse, vorhandene Standards und Richtlinien sowie das Sicherheitsbewusstsein der Mitarbeiter. Tests erfolgen durch Interviews, etwa mit Sicherheitsverantwortlichen, Systemadministratoren und der Personalleitung.

Zertifikat wird bald zur Pflicht

Der Erfolg der Programme hängt davon ab, dass sich alle Partner anschließen und die Überprüfungen korrekt vollziehen. VISA und MasterCard schreiben die Zertifizierung denn auch zwingend vor und planen gegen unwillige Partner Sanktionen, die von Haftungsklagen bis hin zum Ausschluss von der Kreditkartenabwicklung reichen können. So weit muss es aber nicht kommen, denn von mehr Sicherheit im Online-Handel profitieren letztlich alle Beteiligten. „Für Online-Shops bietet sich jetzt die Möglichkeit, durch eine frühzeitige Zertifizierung gleichsam Werbung in eigener Sache zu betreiben und sich gegenüber dem Wettbewerb als Unternehmen zu profilieren, das die Sicherheitsbedenken seiner Kunden Ernst nimmt“, empfiehlt Thorsten Schröter, der bereits einige PCI-Zertifizierungen begleitet hat. Aus dieser Perspektive bieten die neuen Sicherheitsstrategien eine Menge Potenzial, das Thema „Zahlen im Internet“ mittelfristig in den Hintergrund zu drängen. Dem Onlinehandel wird dies weitere positive Impulse verleihen.