

Wie Sparkassen im hart umkämpften Bankenmarkt bei Kunden punkten können

# Datensicherheit wird zum Verkaufsargument

Datensicherheit gewinnt als Verkaufsargument im hart umkämpften Bankenmarkt immer mehr an Relevanz. Schon für 2009 rechnet das Bundeskriminalamt beim Phishing, also dem illegalen Abgreifen von Bankkunden- und Kreditkarteninformationen im Internet, mit einem Anstieg von bis zu 40 Prozent. Innerhalb der nächsten drei Jahre wollen sich daher drei von fünf deutschen Sparkassen und Banken gegenüber dem Kunden als sicherste Bank profilieren. Denn für Kunden wird es bei der Auswahl eines Finanzdienstleisters immer schwieriger, die Geldhäuser in ihrem Produktportfolio voneinander abzugrenzen. Datensicherheit als Abgrenzungsmerkmal im Wettbewerb avanciert also künftig zum Top-Vertriebsthema. Das ist das Ergebnis der Studie „IT & Vertrieb in der Bankenwirtschaft 2009“ des Beratungs- und Softwarehauses PPI AG.

THOMAS REHER

Der Schutz sensibler Daten vor Missbrauch ist ein überzeugendes Vertriebsargument, denn Privat- und Geschäftskunden erwarten insbesondere bei ihrem Finanzdienstleister Sicherheit und Zuverlässigkeit. Werden erst einmal Manipulationen in der Öffentlichkeit bekannt, sind die Imageschäden für das Kreditinstitut folgenreich. Das sensible Vertrauensverhältnis zum Kunden wird belastet und endet im schlimmsten Fall damit, dass der Kunde sich einem seiner Meinung nach vertrauenswürdigeren Institut zuwendet. Sparkassen, die Datensicherheit zu ihrem Top-Vertriebsthema erkoren haben, sind für enttäuschte Anleger dann besonders attraktiv. Ein Mehr an Sicherheit lassen sich Bankkunden sogar gern etwas kosten: Jeder zweite Kontoinhaber nimmt Zusatzkosten in Kauf, wenn dadurch die Bankgeschäfte im Internet besser geschützt werden.

Schon jetzt messen mehr als 40 Prozent der Sparkassen und Banken dem Thema Sicherheit große Bedeutung für den Unternehmenserfolg bei. Nur das Kundenbeziehungsmanage-



Im Internet tummeln sich zahlreiche Kriminelle, die weltweit auf Datenklau gehen. Besonders für Kreditinstitute gilt: Nur wer bei der Sicherheitsausstattung ganz vorne mitspielt, gewinnt das Vertrauen der Kunden. Foto: dpa

ment hat noch mehr Einfluss. Die Datensicherheit ist aber der Bereich, der innerhalb der nächsten drei Jahre am stärksten an Relevanz gewinnen wird. IT-Lösungen zur Sicherung von Bank- und Kontoinformationen werden in Zukunft fast genauso wichtig eingestuft wie eine effektive Kundenmanagementsoftware. Hinzu kommt, dass die Sicherheit auch den Ansprüchen der zunehmenden Mobilität im Zahlungsverkehr gerecht werden muss. Bank-

kunden wollen ihren Kontostand im Internet unabhängig vom Aufenthaltsort abfragen oder Überweisungen unterwegs tätigen – und das möglichst sicher. Online-Banking genießt auch bei den Bankentscheidern unter den Vertriebskanälen im Privatkundenbereich die stärkste Aufmerksamkeit. Um dabei ein Höchstmaß an Sicherheit zu gewährleisten, investieren die Sparkassen verstärkt in IT-Schutzmaßnahmen für das Mobile Banking.

Die Sparkassen sind die erste Finanzgruppe, die eine mobile Banking-Applikation für das iPhone und den iPod Touch entwickelt hat. Sicherheit steht dabei an erste Stelle: Die Schnittstelle zum Kreditinstitut wird per TAN-Verfahren verschlüsselt und die Kontodaten über eine Weiterentwicklung des Standards HBCI abgerufen. Die verschlüsselten Informationen werden ohne Umwege direkt zwischen iPhone und Sparkasse ausgetauscht. Zudem entwi-

ckeln die Sparkassen stetig ihre TAN-Verfahren in Kombination mit Chipkarten weiter. So planen sie beispielsweise die bundesweite Einführung der „chipTAN comfort“. Bei diesem Verfahren erkennt ein optisches Lesegerät die Auftragsdaten wie Kontonummer oder Überweisungsbetrag und generiert eine einmal gültige TAN. Das ersetzt die iTAN-Liste in Papierform.

Auch im Firmenkundengeschäft bieten Sicherheitsaspekte im Zahlungsverkehr wichtige Vertriebsansätze. Unternehmen forderten von den Geldhäusern browserbasierte, multibankfähige Lösungen, die den sicheren Datenaustausch ermöglichen. Mit dem neuen Zahlungsstandard EBICS hat die Kreditwirtschaft diese Anforderungen erfüllt. Seit 2008 kommen die Unternehmen in den Genuss eines erhöhten Sicherheitsniveaus beim Datenaustausch im Internet.

Moderne Verschlüsselungsverfahren mit zusätzlichen Signaturen ermöglichen nicht nur den europaweiten Zahlungsverkehr, sondern sorgen auch mit einer starken Authentifizierung für einen sicheren Schutz der Kontodaten. Zudem können Aufträge, ganz im Sinne der Mobilität, bei Bedarf standortunabhängig freigegeben werden. Bei der Entstehung von EBICS nehmen die Sparkassen eine Vorreiterrolle ein: Das Informatikzentrum der Sparkassenorganisation (SIZ) hat die Entwicklung des Zahlungsstandards angeregt und von Beginn an mitgeprägt.

Fazit: Die Sparkassen haben erkannt, dass die Sicherheit im Electronic Banking sich vom Wirtschaftlichkeits- und Kostenfaktor zum strategischen Geschäftsfeld entwickelt. Verbesserte Sicherheitsmaßnahmen stellen einen starken Treiber für künftige Geschäftserfolge dar und dienen aktiv der Kundenbindung und dem Ertrag. Sowohl für Privat-, als auch für Geschäftskunden steht der Schutz sensibler Daten im Zuge der Mobilität immer mehr im Vordergrund und kann letztlich bei der Auswahl des Finanzdienstleisters wettbewerbsentscheidend sein.

Der Autor ist Vorstand der PPI AG Informationstechnologie in Kiel