Informationssicherheit für Marketing nutzbar

Von Roland Bubik und Christian Beekes

Kriminelle Attacken gegen Banken und ihre Kunden nehmen immer professionellere Dimensionen an. Dementsprechend aufmerksam sind die Kunden geworden, wenn es um das Thema Datensicherheit geht. Für die Institute ergeben sich dadurch neue Möglichkeiten: Wer besondere Sicherheit im Datenverkehr bietet, kann das Thema auch fürs Marketing nutzen, meinen Roland Bubik und Christian Beekes. Red.

Informationssicherheit im Bankgeschäft rückt zunehmend in den Fokus. Lücken in diesem Bereich bedeuten für Finanzdienstleister nicht nur handfeste betriebswirtschaftliche Kosten. „Sicherheit" entwickelt sich vielmehr zu einem eigenständigen Kriterium im Wettbewerb. Aktuelle Fakten unterstreichen diese neue Relevanz von Informationssicherheit im Bankgeschäft:

- 50 Prozent der deutschen Internet-Nutzer lehnen aus Sicherheitsbedenken das Online-Banking ab (Forrester).

- 1,5 Millionen Bankkunden in Europa haben laut eigenen Aussagen aus mangelnder Sicherheit das Online-Banking aufgegeben (Forrester).

- Die Mehrheit der Retail-Banking-Kunden stuft Sicherheit wichtiger ein als andere zentrale Leistungsmerkmale wie etwa ein breites Produktangebot, freundliches Bankpersonal oder Erreichbarkeit der Filialen (Booz Allen Research).

- Mehr als ein Drittel der Kunden wäre bei überlegener Sicherheitstechnik bereit, die Bankbeziehung zu wechseln (Booz Allen Research).

- Die Anzahl von Phishing-Attacken in Deutschland hat in den letzten sechs Monaten um über 50 Prozent zugenommen, wobei von einem direkten Schaden für die deutsche Kreditwirtschaft in der Größenordnung von 20 bis 25 Millionen Euro für 2006 ausgegangen werden kann. Ohne Gegenmaßnahmen wird dieser Schaden auf 75 bis 80 Millionen Euro jährlich anwachsen (Booz Allen Research). (Siehe Abbildung 1)

- Hinzu kommen indirekte Einbußen, die noch einmal deutlich über diesen Werten liegen können. Diese Einbußen resultieren vor allem aus der schwächeren Nutzung des margenstarken Online-Bankings, welches die Kunden aufgrund von angenommenen Sicherheitslücken scheuen. Schätzungen beziffern die Einbußen daraus auf etwa 70 Millionen Euro pro Jahr (Booz Allen Research).

Zu den Autoren

Roland Bubik ist Mitglied der Geschäftsleitung, **Christian Beekes** ist Senior Associate bei Booz Allen Hamilton, München.

Banken von organisierter Kriminalität bedroht

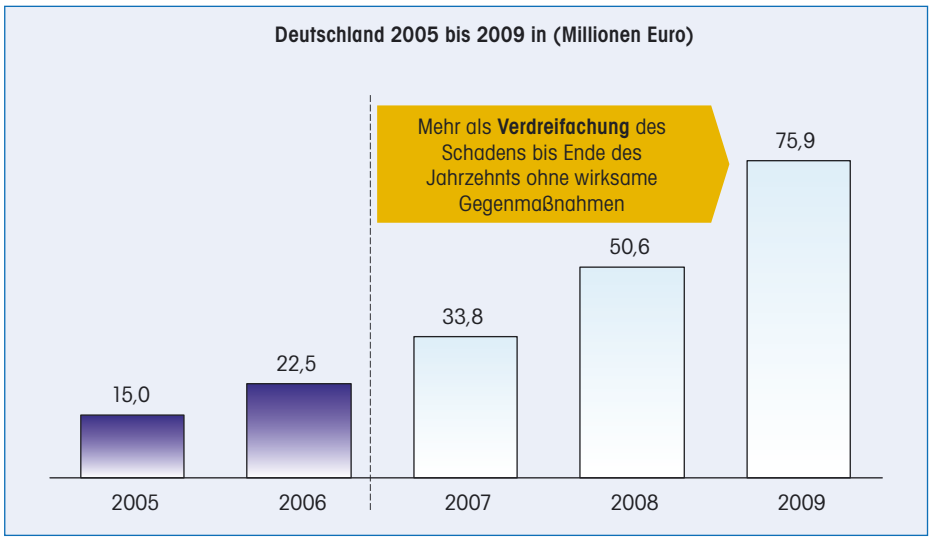
Die Bedenken der Bankkunden sind berechtigt. Die Sicherheitsattacken haben mittlerweile eine neue Qualität erreicht. Längst sind es nicht mehr nur die privaten Hacker, die vom heimischen PC aus ihr Unwesen treiben.

Banken werden heute von organisierter Kriminalität bedroht, die sich intelligenter und flexibler Methoden bedient, etwa dem Einschleusen von Personal, um in Call-Centern von innen heraus Manipulationen vorzunehmen. Auch vollspezifizierte Kreditkartennummern werden zur missbräuchlichen Verwendung angeboten.

Abwanderung von Kunden droht

Nachdem vor einigen Jahren vor allem englischsprachige Länder betroffen waren, wird nun auch Deutschland verstärkt zur Zielscheibe von kriminellen Attacken. Diese richten sich in erster Linie auf die Online-Aktivitäten. Weitere sensitive Kanäle und Produkte sind das Telefon-Banking sowie Debit- und Kreditkarten (siehe Abbildung 2). So sehen sich zahlreiche Banken einem vielfältigen Gefahrszenario ausgesetzt:

Abbildung 1: Ohne wirksame Gegenmaßnahmen wird sich der direkte Schaden von Phishing-Attacken bis 2009 verdreifachen



- Unmittelbarer betriebswirtschaftlicher Schaden durch Betrugsfälle, missbräuchliches oder manipulatives Verhalten,
- Verschlechterung der Kostenposition durch unzureichende Ausnutzung der effizienten Vertriebskanäle Online und Telefon,
- Kundenverlust durch Abwanderung betroffener Kunden und
- Imageverluste.

Breiteres Verständnis von „Banking Information Security"

Um dem skizzierten Sicherheitsrisiko entgegen zu treten, ist ein breites Verständnis von „Banking Information Security" zu empfehlen, das alle Sicherheitsaspekte umfasst:

- Betrug und Missbrauch („Fraud"),
- Verfügbarkeit der Kanäle, Funktionen und Services („Availability"),
- Vertraulichkeit („Confidentiality"),
- Integrität und Fehlerlosigkeit („Integrity and Certainty").

Hierbei empfiehlt sich ein zweistufiges Vorgehen: Auf der ersten, eher „defensiven Stufe" steht die Minimierung von Sicherheitsrisiken als entscheidender Punkt. Auf der zweiten, „offensiven Stufe" rückt die Marketing-Nutzung der eigenen, verbesserten Positionierung zum Thema Sicherheit ins Zentrum. (Siehe Abbildung 3)

Erste Stufe: Gefahrenabwehr

Die erste Stufe richtet sich darauf, die Gefahrenabwehr zu verbessern, die direkten Schäden zu minimieren und den Umgang mit Sicherheitsfragen zu professionalisieren. Bereits hier ist das Thema „Banking Information Security" ganzheitlich zu verstehen und anzugehen. Es umfasst Maßnahmen in den Bereichen (Informations-) Technologie, Operations/Prozesse, Policies/Standards, Organisation, Personal. In Frage kommen beispielsweise:

- Zur Phishing-Abwehr: Transaktionsprofile und spezialisierte Werkzeuge, die das Auslesen von Daten verhindern,
- „Virtuelle Kreditkarten" für den Karten-Einsatz im Web,
- Personalauswahl und laufendes Screening im Telefonbanking,
- Risiko-Management-Framework und -Prozesse zur Risiko-Prognose, Risiko-Validierung und -Abwehr.

Zweite Stufe: Sicherheit als Wettbewerbsvorteil

Auf der zweiten Stufe können Fortschritte im Bereich ganzheitlicher Sicherheitslösungen genutzt werden, um „Banking Information Security" in eine marktseitige „Security Value Proposition" der Bank einzubinden. Damit wird sie zum echten und aktiv vermarkteten Wettbewerbsvorteil.

Abbildung 2: Der Kartenbetrug durch elektronische Kanäle nimmt gegenüber dem physischen Betrug am Point-of-Sale deutlich zu

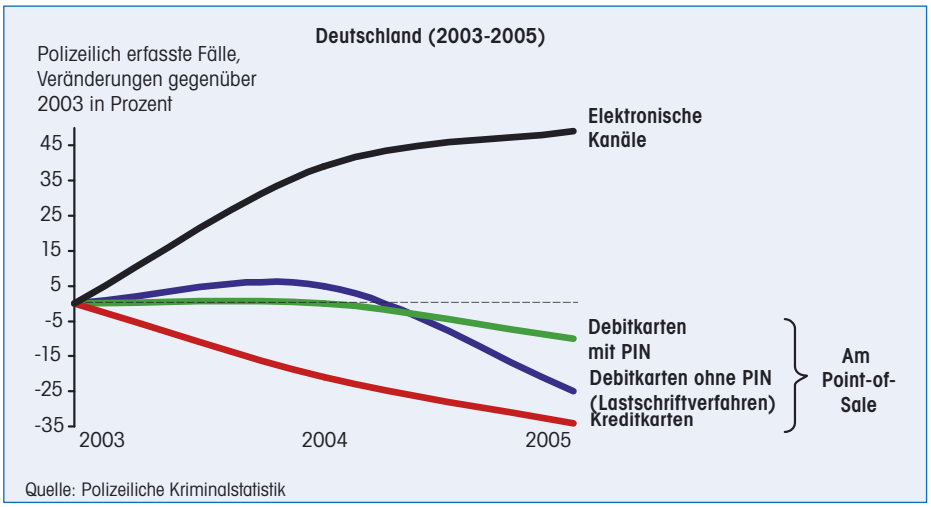
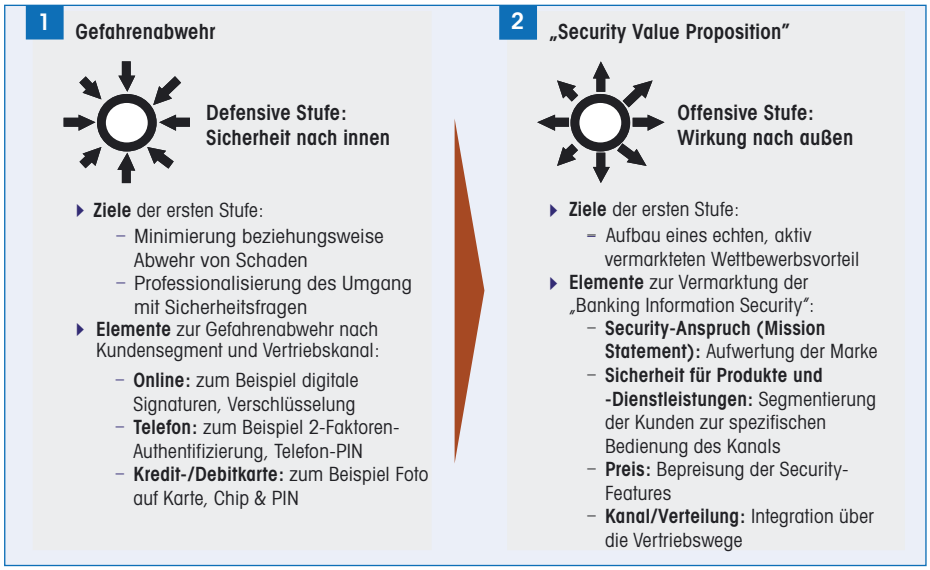


Abbildung 3: Die Phasen der Einführung einer erfolgreichen „Banking Information Security" haben klar definierte Ziele



Zu einer solchen Information „Security Value Proposition" gehören – auf der Basis einer gefundenen technologischen, operativen, organisatorischen und personellen Lösung – die Einbindung und Nutzung des Themas in den Bereichen Marketing, Kommunikation, Produktentwicklung, Kundensegmentierung und Anpassung des Sicherheitsangebotes, Pricing und Vertriebskanalmanagement.

Marketing: Wie angelsächsische Banken vormachen, kann „Sicherheit" (als Gegenpart zum „Risiko") emotional aufgeladen und als „Brand Message" in den Markt getragen werden – bis hin zu einem entsprechenden Logo.

Kommunikation: Gegenüber Analysten, Investoren, Kunden und anderen Marktteilnehmern/Beobachtern sollte das Thema Sicherheit in allen Kommunikationskanälen angemessen besetzt werden. Auch auf diese Weise entsteht ein „Brand Claim" für „Sicherheit".

Produktentwicklung und Kundensegmentierung: Finanzdienstleister müssen beginnen, ihre Produkte für die sicherheitsorientierte Klientel entsprechend auszugestalten. Gerade im Zahlungsverkehr bestehen entsprechende Produktdifferenzierungsmöglichkeiten (zum Beispiel digitale Signaturen im Online-Bereich, Zwei-Faktoren-Authentifizierung im Telefon-Banking). Damit können neue Kundenschichten angesprochen und bestehende Kunden bedürfnisgerechter bedient werden.

Pricing: Wo Wertschätzung für Sicherheit besteht, kann auch über die Bepreisung besonderer Sicherheitsleistungen nachgedacht werden – mit direkten Implikationen für die Erlössituation.

Wie das Risiko gehört auch die Sicherheit zum Geschäft der Bank. Wer Sicherheit lediglich als Thema des IT-Security-Beauftragen versteht, greift zu kurz. Auf der Gefahrenabwehrseite sind ganzheitliche Ansätze über die verschiedenen Bedrohungsbereiche und -quellen hinweg zu definieren.

Erst eine proaktive „Vermarktung" von Sicherheit als Teil der „Security Value Proposition" erschließt jedoch das komplette Potenzial von Sicherheitslösungen und nutzt die entsprechenden Investitionen optimal. Damit sind Banken gerüstet für eine Welt, in der die gesellschaftliche und wirtschaftliche Stellung des Themas Sicherheit auf allen Ebenen eklatant zunimmt. ■