Safety First

Marktpositionierung von Banken mittels Informationssicherheit

Erschienen in DMR Onlineportal, 20.07.2009

Christian Frefel
Dr. Laura Georg

Eine aktuelle europäische Studie der Managementberatung Detecon (Schweiz) AG zeigt, wie und in welchem Ausmaß Bankinstitute von einer Erhöhung des Kundenvertrauens in die Sicherheit ihrer Online-Banking-Systeme profitieren können.

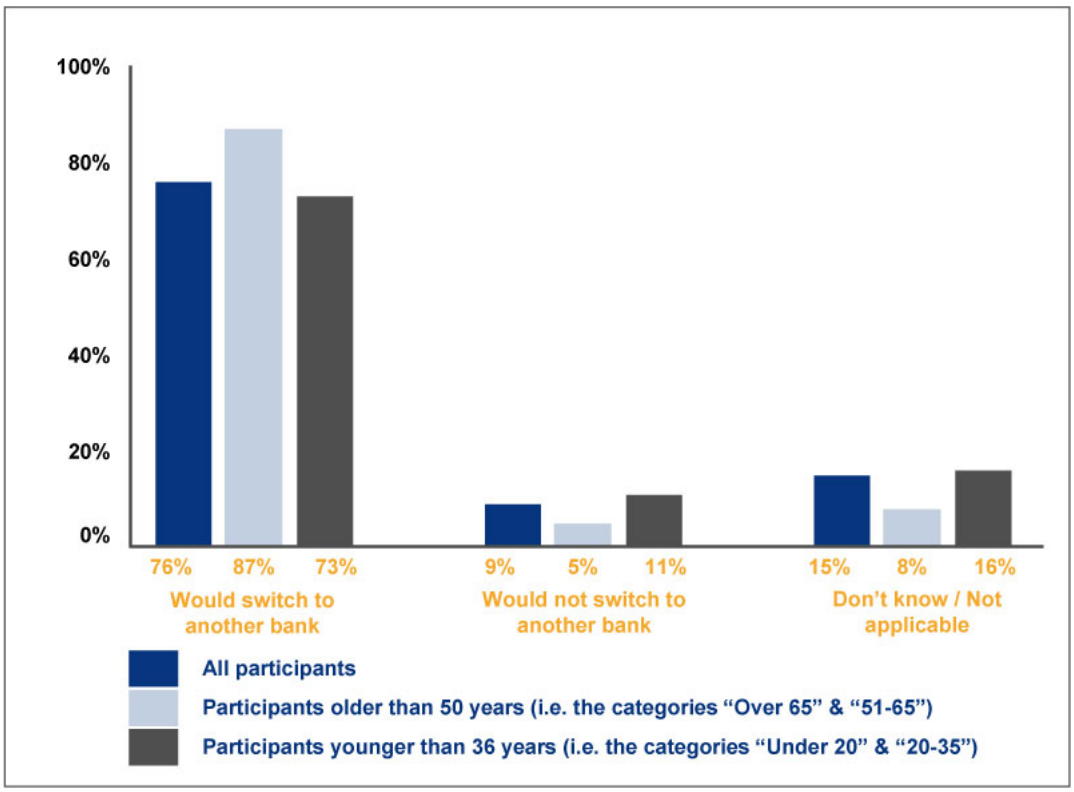
Online-Banking wurde in den letzten Jahren aufgrund seiner attraktiven Kostenstruktur zu einem immer profitableren Geschäft für den Bankensektor. Gleichzeitig gingen mit dieser innovativen Art, Bankgeschäfte zu tätigen, auch bisher nicht gekannte Herausforderungen für die Sicherheit mit einher (*Vgl. z. B. BSI (2008)*). Basierend auf vorausgehenden Studien und in Kooperation mit Forschern dreier renommierter europäischer Hochschulen - London (LSE), Graz (TU) und Luzern (HTA) - wurde die Meinung von knapp 400 Bankkunden erhoben und 18 Interviews mit Sicherheitsmanagern im Bankensektor geführt, das heißt mit Chief Information Security Officers (CISO), anderen Verantwortlichen für Informationssicherheit und Beauftragten für Online-Banking aus der Schweiz, Österreich, Deutschland, Frankreich, England und den Niederlanden (*Vgl. Liebenau und Kärrberg (2006), S. 51ff und Georg (2007) S. 321ff*).

Sicherheitsbedenken und die Sensibilität der Bankkunden

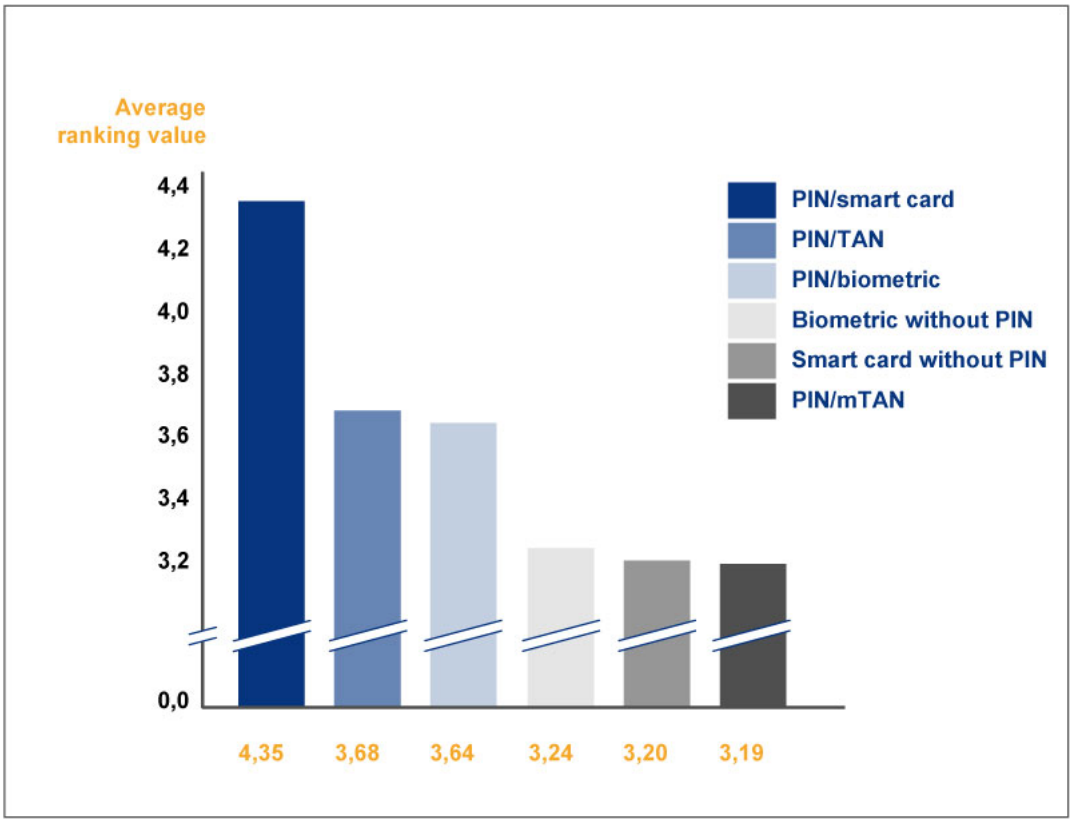
Nicht zuletzt die Wellen von Phishing-Mails in den letzten Jahren sind dafür verantwortlich, dass unter den Verbrauchern eine nicht zu unterschätzende Skepsis herrscht. 82 Prozent der Umfrageteilnehmer, die Online-Banking nicht nutzen, gaben an, dass Sicherheitsbedenken bei ihrem Verzicht eine Rolle spielt. Auch das Vertrauen von bestehenden Online-Banking-Nutzern könnte noch deutlich erhöht werden: 46 Prozent aller Online-Banking-Nutzer schätzen die Wahrscheinlichkeit, dass eine unbefugte Person über

Sicherheitslücken des Online-Bankings Kontoinformationen einsehen kann, als „mittel“ oder sogar höher ein. Auch gaben 45 Prozent der Umfrageteilnehmer die eigene Ungewissheit über das Risikopotenzial oder Unachtsamkeit als Grund an, Online-Banking nicht zu nutzen. In diesem Zusammenhang ist ebenfalls der hohe Informationsbedarf zu sehen, den die Umfrage aufdeckte: Rund 60 Prozent der Teilnehmer möchten besser über Sicherheitsmassnahmen informiert werden. Ein gleich großer Anteil der Befragten interessiert sich für Rankings, die Bankinstitute nach ihrem Sicherheitsniveau ordnen. In der Gruppe der über 50-Jährigen beträgt dieser Anteil sogar rund 80 Prozent.

Bankinstitute, die der vorhandenen Skepsis erfolgreicher als andere begegnen, dürfen nicht nur mit einer höheren Durchdringungsrate des Online-Bankings rechnen, sondern auch mit einem signifikanten Neukundenzuwachs. 43 Prozent der befragten europäischen Bankkunden sehen den Faktor „Informationssicherheit“ als „sehr wichtig“ oder „wichtig“ in ihrer Entscheidung für eine bestimmte Bank. 76 Prozent wiederum würden das Bankinstitut wechseln, wenn sie in Kenntnis einer Mehrzahl von aktuellen Fällen gelangten, bei denen Unbefugte Zugriff auf sensible Informationen erhielten.



Sicherheitsmassnahmen auf der Bank- und Kundenseite Die interviewten Experten sind sich der Bedeutung der Informationssicherheit jedoch bewusst und zeigen Investitionsbereitschaft. Gefordert, vielfach bereits umgesetzt oder in Planung ist beispielsweise die Schaffung einer CISO-Funktion, die sich nicht nur auf technischer, sondern auf ganzheitlicher Ebene mit dem Thema auseinandersetzt. Während die meisten Sicherheitsanstrengungen der Bankinstitute im Hintergrund und damit für den Kunden „unsichtbar“ ablaufen, sind es vor allem die Methoden zum Einloggen in das Online-Banking und zur Authentisierung von Transaktionen, die stark sicherheitsrelevant und im Fokus der Wahrnehmung des Kunden stehen. Die Umfrage ergab, dass ein System mit PIN und Chipkarte den meisten Anklang findet, noch vor der herkömmlichen PIN/TAN-Methode mit Streichliste. Bemerkenswert ist, dass auch die in den Medien umstrittenen biometrischen Methoden in punkto Beliebtheit bei den Befragten gut abschneiden. Diese Methoden werden jedoch bisher noch von fast keiner europäischen Bank eingesetzt. Als eher unbeliebt erwies sich die mTAN-Methode, das heißt die Authentisierung mittels eines Codes, der dem Nutzer per SMS zugestellt wird. Hier unterscheiden sich jedoch die europäischen Konsumenten. Betrachtet man nur die österreichischen Teilnehmer, rangierte diese Methode jedoch gerade zuoberst auf der Beliebtheitsskala, was möglicherweise auf den breiten Einsatz dieser Technologie in Österreich zurückzuführen ist. Einmal im Einsatz erscheint diese Authentifizierungsmethode für Kunden überzeugend.



Nicht nur die Bank steht in der Pflicht, die angebotenen Internet-Dienstleistungen möglichst sicher zu gestalten, auch der Kunde muss entsprechend handeln. So ist es die Pflicht des Konsumenten, einen sorgfältigen Umgang mit Passwörtern zu pflegen oder die jeweils aktuelle Version eines Virenscanners zu verwenden. Wie weit ein Normalverbraucher in die Sicherheitsverantwortung gezogen werden kann, wird kontrovers diskutiert und wurde in einzelnen Fällen sogar schon zum Gerichtsfall (*Vgl. z. B. Karper (2006) und der Gerichtsbeschluss des Landgerichtes Köln 9 S 195/07 vom 05.12.2007 („Kein Mitverschulden eines Phishing-Opfers“)*). Gemäß der Studie sieht eine Mehrzahl - 74 Prozent der europäischen Bankkunden - „primär“ sich oder „eher“ sich als die Bank in der Verantwortung sieht, den eigenen Computer so auszurüsten, dass vom Zustand dieses Gerätes her keine realistische Gefahr mehr droht. Im Hinblick auf die

Bereitschaft der Kunden, Verantwortung zu übernehmen, waren deutliche regionale Unterschiede festzustellen. So antworteten 42 Prozent der Briten, die an der Umfrage teilgenommen haben, es sei „eher die Bank“ oder sogar „primär die Bank“, die für die Sicherheit des eigenen Computers verantwortlich zu machen wäre.

Kompensationsforderungen an die Bank

Während die interviewten Sicherheitsexperten größtenteils angenommen haben, dass im Schadensfalle - auch wenn dieser erst durch eine (grobe) Nachlässigkeit des Kunden entstanden ist - Kulanz von der Bank gefordert wird, zeigte die Umfrage, dass die Konsumenten diesbezüglich meinungsheterogener sind. Die Umfrage bezog sich dabei auf einen hypothetischen Schadensfall, der durch einen Zugang zum Online-Banking über ein unsicheres, öffentliches Netz ermöglicht wurde. Nur 18 Prozent der Kunden, die sich in der Verantwortung für die PC-Sicherheit sehen, fordern eine Entschädigung der Bank, wenn bei ihnen ein klares Fehlverhaltens identifiziert werden kann. Kunden, die die Bank in der Verantwortung für die Sicherheit des eigenen PCs sehen, verlangen im Gegenzug mit einem Anteil von 64 Prozent auch dann eine Entschädigung, wenn sie selbst ungenügende Vorsicht walten ließen.

Kundenfreundliche Informationssicherheit schafft einen Mehrwert

Was die Entwicklung der Sicherheitssituation angeht, so sind Kunden und Experten interessanterweise unterschiedlicher Meinung. Während eine klare Mehrheit von 68 Prozent der befragten Konsumenten der Meinung ist, Online-Banking sei in den letzten fünf Jahren sicherer geworden, betonten die interviewten Bankexperten vor allem die Bedrohung durch die organisierte Kriminalität, die in den letzten Jahren zugenommen habe und weiter zunehmen werde.

Insgesamt zeigt die Studie, dass Bankinstitute von state-of-the-art Sicherheitsmassnahmen, die den Kunden gut kommuniziert werden können und kundenfreundlich aufgebaut sind, in vielerlei Hinsicht nachhaltig profitieren können. Die Herausforderung bleibt dabei, die Wünsche der Kunden zu berücksichtigen, um sichere Produkte anzubieten, die durch Kundenakzeptanz honoriert werden.

Literatur

Deutsches Bundesamt für Sicherheit in der Informationstechnik, Lagebericht 2008, 2008, S. 24.

Laura Georg, The Function of Corporate Security within Large Organisations – The Interrelationship between Information Security and Business Strategy, Université de Genève, Genf, 2007, S. 321 ff.

Landgericht Köln, Urteil 9 S 195/07 von 05.12.2007, http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2007/9_S_195_07urteil20071205.html, besucht am 06.03.2009.

Jonathan Liebenau & Patrik Kärrberg, International Perspectives on Information Security Practices: Opinions, Preferences and Tools in the Financial Services Industry, London School of Economics and Political Sciences, 2006, S. 51 ff. Irene Karper, Sorgfaltspflichten beim Online-Banking - Der Bankkunde als Netzwerkprofi?, Datenschutz und Datensicherheit, Vol. 30, Nr. 4, April 2006, S. 215-219.

Christian Frefel
Christian Frefel hat als Teammitglied bei der Detecon Schweiz am Design, der Analyse und Dokumentation der Studie "The Value of Information Security to European Banking Institutions" mitgearbeitet. Er kann auf mehrere Jahre Erfahrung in der Consultingbranche zurückblicken und hat sich in diesem Rahmen insbesondere längere Zeit mit dem ISO-27001-Informationssicherheitsstandard beschäftigt.

Dr. Laura Georg
Dr. Laura Georg leitet das Information Security Management Team der Detecon (Schweiz) AG. Während ihrer Beratertätigkeit hat sie sich auf dem Gebiet der Mehrwertschaffung für Unternehmen durch die Optimierung des Informationssicherheitsmanagements spezialisiert. Sie verfügt über eine langjährige Erfahrung in den Gebieten Information Security Governance, IT Risk Management und Information Security Compliance.