

Sicherheit ist vor allem eine Frage des Betriebs

Die Bankkunden von heute wollen mit ihrer Bank auch ausserhalb der Öffnungszeiten via Internet kommunizieren. Diese Erwartungshaltung stellt vor allem kleinere und mittlere Finanzinstitute vor neue Herausforderungen, insbesondere im Bereich der Sicherheit. *Kaspar Geiser*



Kaspar Geiser
ist Managing Director und
Mitinhaber der Aspectra AG

Bevor technische Fragen erörtert werden, muss sich die Bank überlegen, welche Dienstleistungen den Kunden überhaupt online angeboten werden sollen. Hier ist eine ganze Bandbreite von der blossen Abfrage von Finanzinformationen bis zur Online-Börsentransaktion denkbar. Der elektronische Kanal muss die konventionellen Kanäle, insbesondere die Kundenberatung, unterstützen und nicht konkurrieren. Es muss von Beginn an sichergestellt sein, dass der Kundenberater über alle durch den Kunden im Internet getätigten Aktionen informiert ist und bei Bedarf eingreifen kann.

Die enge Verknüpfung zwischen E-Banking und Kundenbetreuung stellt wiederum die Frage nach den «Öffnungszeiten» des E-Banking, genauer: nach der Reaktionszeit auf etwaige Anfragen oder Aufträge. Auch muss die Frage des Supports, also des Helpdesks für E-Banking-Anwendungen, vor und nicht während oder sogar nach der Umsetzung eines solchen Projektes bestimmt werden. All diese Fragen sind strategischer Natur und müssen von der Bank geklärt und definiert werden.

Entwicklung und Betrieb sind zwei paar Schuhe

Ausgehend von den definierten Zielen müssen die nötigen Voraussetzungen für die «technische» Umsetzung geschaffen werden. Dies stellt bereits erste technische Anforderungen. Welche Core-Systeme meiner Bank sind für die Erbringung der E-Banking-Funktionen nötig? Was sind die Betriebszeiten dieser Systeme? Wie sicher sind diese Systeme? Wer betreut diese Systeme? Wie verläuft der Informationsfluss zwischen Kunde, Kundenbetreuung und den Core-Systemen? Welche zusätzlichen Systeme sind zum Betrieb einer

E-Banking-Anwendung nötig? Welche Risiken bestehen, wenn Teile des Bankgeschäfts online zur Verfügung stehen?

Die Entwicklung und der Betrieb von E-Banking-Anwendungen sind zwei paar Schuhe. Stehen während der Entwicklung Themen wie Funktionen, Layout, Testing im Vordergrund, sind Fragen wie Verfügbarkeit, Sicherheit und Performance Sache des Operatings. Insbesondere die Frage nach möglichen Si-

cherheitsmechaniken sollte keinesfalls «nur» von der Entwicklung gestellt und beantwortet werden, sondern auch nach der Umsetzung – und dies permanent. Unter

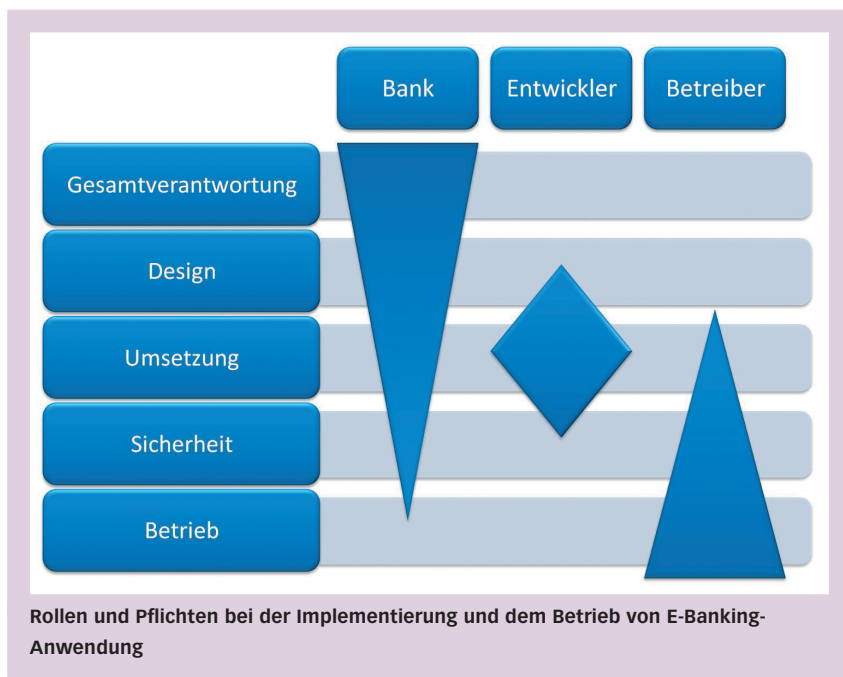
diesem Aspekt ergibt es Sinn, dass sicherheitsrelevante Elemente einer E-Banking-Anwendung vom Betreiber realisiert und betreut werden.

Die Schulung ist nicht zu vernachlässigen

In der Verantwortung der Entwicklung steht somit die Umsetzung der gewünschten Funktionen. Die diesen Funktionen zugrunde liegenden Bankprozesse müssen von den Entwicklern verstanden und gemäss dem Geschäftsmodell umgesetzt werden. Diktiert die Technik dem Geschäft Prozesse und Vorgehensweisen, wird es schwierig, die nötige Akzeptanz für E-Banking-Anwendungen innerhalb der Bank zu finden.

Auch die Schulung aller bankinternen involvierten Stellen muss innerhalb der Entwicklung stattfinden. So ist es der realisierenden Partei möglich, auf Wünsche und Fragen einzugehen und die Abläufe noch besser zu verstehen. Dies sollte mit jeder neuen Version einer E-Banking-Anwendung wiederholt werden. Der Entwicklungsprozess verlangt somit nach sowohl technisch versierten wie aber auch beratenden und didaktisch fähigen

«E-Banking-Anwendungen sind technische und logistische Herausforderungen.»



gen Mitarbeitern. Eine optimale Usability erfordert zudem die Mitarbeit kreativer Köpfe in der Entwicklung, damit die gestellten Anforderungen sowohl ergonomisch sinnvoll, wie auch in ansprechendem Design realisiert werden.

Hohe Anforderungen an den Betrieb

Wie bereits erwähnt, ist es sinnvoll, neben dem reinen Betrieb einer E-Banking-Anwendung auch die sicherheitsrelevanten Aufgaben ein und derselben Partei zuzuordnen. An dieser Stelle daher eine kurze Umschreibung, was zu sicherheitsrelevanten Aufgaben und Komponenten gezählt wird. An erster Stelle stehen sicherlich die Firewalls und die Verbindungen vom E-Banking zum Core-System. Diese müssen aktiv betreut werden und dies permanent, also auch ausserhalb der Öffnungs- und Betriebszeiten einer Bank.

Als Nächstes müssen die Systeme und Standardapplikationen aktiv überwacht und im Bedarfsfall mit den nötigen Updates versehen werden. Dazu zählen das Betriebssystem, die Datenbank sowie die unter Umständen vom Entwickler eingesetzten Applikationsserver. E-Banking-Anwendungen verfügen über so genannte starke Authentifizierungsmechanismen. Dies sind neben Benutzername und Passwort Streichlisten, Zertifikate oder dynamische Secrets. Auch diese Komponenten muss der Betreiber zur Verfügung stellen.

Diese Pflichten stellen hohe Anforderungen an das Betriebspersonal und an die

eingesetzten technischen Systeme, die die Schutz- und Sicherheitsfunktionen übernehmen. Insbesondere kleinere, aber auch mittlere Institute verfügen in der Regel nicht über das Personal für den sicheren Betrieb einer E-Banking-Applikation. Aus dieser Überlegung heraus kann es somit sinnvoll sein, dass der Betrieb von E-Banking-Anwendungen Dritten übergeben wird.

Gesamtverantwortung kann nicht ausgelagert werden

Banken, die eine E-Banking-Anwendung umsetzen, müssen sich bewusst sein, dass zwar Dritte eine Applikation entwickeln und betreiben können, dass aber die Gesamtverantwortung bei ihnen bleibt. Das bedeutet, dass sie auch nach der erfolgreichen Umsetzung mit geeigneten Massnahmen sicherstellen müssen, dass die Weiterentwicklung möglich und die betriebliche Sicherheit gewährleistet ist. Dazu zählen das Rapportieren von Fehlern, die akribische Dokumentation aller Änderungs- und Erweiterungswünsche sowie die periodische Überprüfung aller Funktionen und der Sicherheitsinfrastruktur.

Management Cockpits, die sowohl über den Systemzustand informieren als auch Dokumentation und Ticketingsystem beinhalten, können hier alle involvierten Parteien in ihrer täglichen Arbeit unterstützen. Was die Sicherheitsüberprüfung betrifft, ergibt es Sinn, dies wiederum Dritten, in der Umsetzung nicht involvierten Parteien zu übergeben. Diese Aufgabe soll auch von internen und externen Auditoren begleitet werden. ■