

# Reduziert Outsourcing bei Banken die IT-Sicherheit?

von Artur P. Schmidt

Dr.-Ing. Artur P. Schmidt ist Publizist und Herausgeber des Wissensnavigators  
<http://www.wissensnavigator.com>

- Sicherheitslücken aller Orten

Die unmittelbare Verantwortung für den sicheren Einsatz der EDV, für den früher in erster Linie sogenannte Service-Rechenzentren (vor allem im Genossenschaftsbereich) zuständig waren, wurde in den 90 er Jahren zunehmend in die Primärbanken hinein verlagert. Die Anpassung der EDV-Landschaften in den Banken an neue Technologien war notwendig, um den Anforderungen eines sich rasant entwickelnden Marktes der Informationstechnologie nachzukommen und somit langfristig wettbewerbsfähig zu bleiben. Durch Fusionen, Kostensenkungsdruck und Fokussierung auf Kernkompetenzen kehrt sich dieser Verlagerungstrend jedoch teilweise wieder um und es werden immer mehr Sicherheitsdienstleistungen outgesourct. Der Trend zum Outsourcing führt in Kombination mit der exponentielle Zunahme der Angriffe von Cyberkriminellen allerdings auch zu immer mehr Sicherheitslücken in den Netzwerken der Banken. Durch den Einsatz neuer IT-Technologien, insbesondere durch den zunehmenden Einsatz von Personalcomputern und deren Vernetzung, haben sich für die Banken neue Aufgaben ergeben wie z.B. das Home-Banking, der Webaufttritt der Bank, der Zugang zum Internet für die Mitarbeiter oder der E-Mail-Verkehr über das Internet. Gleichzeitig sind die Risiken durch externe Hackerangriffe mit Trojanischen Pferden, den allzu sorglosen Umgang von Bankangestellten mit ihren persönlichen Kennwörtern oder die bewusste Datenmanipulation durch Angestellte eines ausgegliederten Rechenzentrums erheblich gestiegen.

- Frühwarnsysteme verbessern

Es gilt im Rahmen der IT-Sicherheit der Unversehrtheit der Daten, der Vertraulichkeit der Daten, der Verfügbarkeit der Daten, der Authentizität der beteiligten Datentransferpartner und der Verbindlichkeit des Datenaustausches höchste Priorität einzuräumen. Wenn immer mehr "Netzwerke und Großrechner von Externen betreut werden, müssen mögliche Risiken frühzeitig erkannt und Sicherheitsstandards schneller als heute den Bedrohungspotentialen angepasst werden. Immer mehr Banken sourcen heute ihre IT-Abteilungen in Tochterfirmen aus, die zu allem Überfluss auch noch unter erheblichem Kostendruck stehen. Leider hat die IT-Sicherheit im Führungs-Cockpit des Top-Managements keine Anzeigeeinstrumente, weshalb die Risiken von Bank-Managern erst viel zu spät erkannt werden. So konnte vor kurzem eine große Retail-Bank wegen eines Systemausfalls für mehr als drei Stunden auf kein einziges Kundenkonto zugreifen. Zieht sich eine Lösung mehrere Tage hin, kann dies zu einem hohen Schaden bei den Kunden führen, die dann auch sehr schnell grössere Schadensersatzforderungen geltend machen können.

- Der Kostensenkungsdruck nimmt zu

Eine branchenunabhängige Umfrage der Meta-Group hat ergeben, dass in über 60% der Fälle das Outsourcing zu Einsparungen von über 10% der IT-Kosten führt. Neben den Kostenaspekten spielen jedoch vor allem Sicherheitsaspekte und die Verfügbarkeit der IT-Systeme eine besondere Rolle. Viele kleinere Banken stossen, vor allem durch die immer kürzer

werdenden Innovationszyklen, an ihre finanziellen Grenzen, so dass diese an der Nutzung von professionell ausgerüsteten Housing- oder Hosting-Anbietern nicht vorbeikommen. Allerdings werden diese Massnahmen erst dann ergriffen, wenn ein Schadensereignis diese Notwendigkeit offenbart. Die EBK macht den Finanzinstituten mittlerweile nicht ohne Grund die Auflage, dass diese einen Business Continuity Plan erstellen, welcher zusammen mit den Schutzmassnahmen im Bereich der IT durch externe Controller periodisch zu beurteilen ist. Mittlerweile sind einige Banken dazu übergegangen für kleinere Banken Insourcing anzubieten, wie der renommierte schweizerische IT-Experte Walter Altherr betont: *„Es gibt einige Banken, welche sich als Insourcer von IT-Dienstleistungen - oder als sogenannte Transaktionsbanken - im Markt positionieren. Es sind dies heute vor allem die Grossbanken, wie die UBS mit ihrer „Bank for Banks“-Dienstleistung, Märki Baumann & Co, Bank Wegelin, State Street und in etwas weiterer Zukunft wohl dann auch einmal die Bank Vontobel.“*

- Verantwortung kann nicht delegiert werden

Banken, die Insourcing anbieten, nutzen hierbei die dafür erforderliche IT-Infrastruktur auch für die eigenen Bedürfnisse und haben somit die Vorschriften der EBK zu erfüllen. Ob dies für den Outsourcer genügt, bedarf einer eingehenden Analyse, allerdings ist die Vorschrift der EBK unzweideutig: Verantwortung kann nicht delegiert werden. Ein besonders heikler Punkt ist hierbei jedoch, ob Transaktionsbanken ihr System genügend gegen Aussen abschirmen? Frits van der Graaff, Managing Director Schweiz des Datenzentren-Dienstleisters IXEurope glaubt nicht, dass sich der Trend zum Insourcing durchsetzen wird: *„Diese Entwicklung wird eher wieder abnehmen. Ich kann mir dies nur für Kantonalbanken vorstellen, wenn gleiche Plattformen benutzt werden. Aber sogar bei den Kantonalbanken ändert sich das schon wieder...Banken sehen andere Banken eher als Mitwettbewerber und sind sicher nicht begeistert wenn ihre Daten beim Konkurrenz im Rechenzentrum aufbewahrt werden“*.

- Risiko lässt nicht nicht outsourcen

Die IT-Outsourcing wird meist mit Argumenten wie Effizienzsteigerung, Kostensenkung, Innovationsfähigkeit oder Economies of Scope begründet. Der wahre Grund dürfte jedoch ein anderer sein: die hohen Kosten für eine eigenständige IT-Abteilung. Da zu allem Übel IT-Manager noch eine andere Sprache sprechen als Top-Manager, reden die Verantwortlichen oftmals aneinander vorbei. Die obersten Führungskräfte möchten sich nicht mit der IT auseinandersetzen, da sie dieser keine strategische Bedeutung zumessen. Es ist jedoch ein grosser Trugschluss wenn geglaubt wird, dass man mit dem Outsourcing auch das Systemrisiko outsourcen könnte. Risiko lässt sich nicht „outsourcen“! Zwar kann dieses durch Versicherungsverträge oder durch operative Regelungs- und Kontrollmassnahmen abgedeckt werden, aber wenn ein System ausfällt, hat dies immer auch erhebliche Konsequenzen auf das Geschäft eines Unternehmens. Deshalb wird das Risiko immer vom Geschäft getragen und ein Outsourcing des Risikos kann deshalb nicht funktionieren. Im Gegenteil kann das Outsourcing das IT-Systemrisiko sogar noch deutlich erhöhen, wenn die Service-Qualität bei der Auswahl des Dienstleisters nicht ausreichend berücksichtigt wurde. Rechenzentren sind im Unterhalt teuer und stehen im Wettbewerb mit neuen Low-Cost-Anbietern.

- Ein billiger Anbieter kann die teuerste Lösung sein

In gewissem Sinne drängt sich hier ein Vergleich mit den Niedrigspreisanbietern der Airline-Branche auf. Um billig anzubieten müssen auch bei Rechenzentren entsprechende Leistungen reduziert werden. Geschäftskritische Applikationen erfordern jedoch einen hohen Zutrittschutz, hohe Verfügbarkeit und einen entsprechenden Service-Level, wozu Urs Bühler,

Geschäftsführer Schweiz des neutralen Rechenzentrums Interxion, ausführt: „Hier einen billigen Anbieter auszuwählen könnte die teuerste Lösung sein. Auf der anderen Seite können Niedrigpreisanbieter sehr attraktive Preise bieten, insbesondere dann, wenn die Anforderungen nicht sehr hoch sind. Letztendlich entscheidet aber der Kunde welchen Standard er für den Betrieb seiner IT benötigt.“ Durch das Outsourcing werden alle undokumentierten Abstimmungsprozesse und informelle Beziehungen aufgehoben. Diese sind jedoch für das Tagesgeschäft und die Aufrechterhaltung eines reibungsfreien Systembetriebes ausgesprochen wichtig. Viele Outsourcer haben deshalb vor Vertragsunterzeichnung kein Interesse auf diese Probleme hinzuweisen, von denen das Top-Management einer Bank zu allem Überfluss oftmals keine Ahnung hat.

- IT-Risikomanagement ist eine Kernaufgabe

Die gesetzgebenden Instanzen sowie Aufsichtsämter haben wegen der in der Banklandschaft zunehmenden Tendenzen nach Verlagerung bzw. Dezentralisierung von Verantwortlichkeiten im Bereich der Informations-technologie und einem verstärkten Outsourcing von Bankfunktionen die damit verbundenen Risiken und Gefahren für die Institute erkannt und Schutzmaßnahmen vorgeschrieben. So ist eine fortlaufende Überwachung der Leistung des Outsourcing-Partners durch die Bank sehr wichtig. Eine Weiterverlagerung ausgelagerter Tätigkeiten auf Subunternehmer sollte nur mit ausdrücklicher Zustimmung einer Bank erfolgen. Besonders wichtig ist, dass es eine vertragliche Zusicherung der Prüfungsmöglichkeiten beim Dienstleistungsunternehmen durch die Interne Revision der Bank, deren Abschlussprüfer und von Aufsichtsämtern gibt. IT-Risikomanagement sollte deshalb heute als Kernaufgabe des Top-Management begriffen werden. Das Risikomanagement darf nicht blauäugig dem IT-Dienstleister überlassen werden. Vielmehr müssen die IT-Risiken systematisch identifiziert, bewertet und gegebenenfalls Gegenmassnahmen eingeleitet werden. Es liegt auf der Hand, dass eine derartige Aufgabe nicht einer klassischen Stabsabteilung übertragen werden kann. Einer der Vorreiter bei der IT-Sicherheit von Banken ist die Deutsche Bank AG, die bereits auf oberster Ebene ein globales Risk Management für IT-Systeme eingeführt hat.

- Outsourcing richtig begreifen

Leider wird der Begriff Outsourcing oft zu allgemein verwendet. Deshalb sollte immer klar präzisiert werden, um welche Outsourcingform es sich konkret handelt. Nur wer vollständig die Geschäftsprozesse auslagert, wer die ganze Applikationsentwicklung ins Ausland (wie z.B. Indien) verlegt, wer umfangreiche IT-Systeme durch Dritte betreiben lässt, wer Rechenzentrumsleistungen von Dritten bezieht, wer das Security-Monitoring externen Servicefirmen überlässt oder wer Housing-Dienstleistungen nützt, sollte tatsächlich von Outsourcing sprechen. „Wer nur eine branchenübliche Standardlösung für einen Teilbereich, wie beispielsweise ein Risk Management System, einsetzt, wer für ein Projekt sein Entwicklerteam durch externe Fachkräfte verstärkt, den betrachte ich nicht als typischen Outsourcer“ sagt der IT-Berater Walter Altherr. Die Erfahrungen aus den Prüfungen und die Auswertungen verdeutlichen, dass sich eine Risikobeurteilung der gesamten EDV in einer Bank nicht nur aus den "neuen" gesetzlichen und aufsichtsrechtlichen Anforderungen ergibt, sondern dass diese die strategische Positionierung der Bank von wesentlicher Bedeutung sind. Damit das Steuerungssystem einer Bank funktioniert, ist es in einer Zeit sich immer schneller verändernden Informationstechnologien und der sich daraus ergebenden gestiegenen Risiken notwendig, sichere Hard- und Software zur Verfügung zu haben.

- Fazit: Auf hohe Verfügbarkeit achten

Die vielerorts als Belastung empfundenen aufsichtsrechtlichen Anforderungen sollten als Chance für die einzelnen Institute gesehen werden. Es besteht kein Zweifel, dass professionelles, bedürfnisgerechtes Outsourcing auch für Banken eine wichtige Rolle einnehmen wird, da es die uneingeschränkte Fokussierung und Konzentration aller Ressourcen auf das Kerngeschäft ermöglicht. Unter Leitungsgesichtspunkten sind die schnelle Verfügbarkeit professioneller Services sowie die Durchführung von IT-Vorhaben ohne betriebsinterne Restriktionen hervorzuheben. Allerdings sollten IT-Outsourcing-Überlegungen nicht aus einem akuten Problemdruck heraus erfolgen, sondern unter Abwägung der Risiken strategisch geplant werden. Der Schlüssel für Banken liegt hierbei vor allem in der Service-Qualität der Anbieter. Einen exzellenten Service bieten heute insbesondere hochverfügbare Rechenzentren, welche nicht nur physisch sondern auch über Firewalls und Intrusion Detection-Massnahmen professionell geschützt sind.

<b>1. In den elektronischen Netzwerken von Banken treten immer mehr Sicherheitslücken auf</b>
<b>2. Insourcing wird sich nur in bestimmten Fällen durchsetzen, da kritische Daten nicht an Dritte ausgelagert werden sollten</b>
<b>3. Risiko lässt sich nicht outsourcen, da das Risiko immer vom Geschäft getragen wird</b>
<b>4. Geschäftskritische Applikationen erfordern einen hohen Zutrittsschutz, hohe Verfügbarkeit und einen entsprechenden Service-Level</b>
<b>5. Eine fortlaufende Überwachung der Leistung des Outsourcing-Partners durch die Bank ist sehr wichtig</b>
<b>6. Eine Weiterverlagerung ausgelagerter Tätigkeiten auf Subunternehmer sollte nur mit ausdrücklicher Zustimmung einer Bank erfolgen</b>
<b>7. Es ist darauf zu achten, dass es eine vertragliche Zusicherung der Prüfungsmöglichkeiten beim Dienstleistungsunternehmen durch die Interne Revision der Bank, deren Abschlussprüfer und von Aufsichtsämtern gibt</b>
<b>8. IT-Outsourcing-Überlegungen sollten nicht aus einem akuten Problemdruck heraus erfolgen, sondern unter Abwägung der Risiken strategisch geplant werden. Der Schlüssel für Banken liegt hierbei in der Service-Qualität der Anbieter</b>
<b>Tab 1: Sum-Up - 8 Schlüsseltrends für das Outsourcing</b>