Banken im Zugzwang

Miriam Veith

Redakteurin

Die deutschen Kreditinstitute standen dem Thema Cloud-Computing aufgrund von Sicherheitsbedenken sowie strengen regulatorischen Anforderungen lange Zeit sehr zögerlich und skeptisch gegenüber. Aber angesichts der allgemein zunehmenden Digitalisierung, den dadurch veränderten Kundenbedürfnissen sowie einem intensiveren Wettbewerb bei Finanzdienstleistungen entstand ein gewisser Zugzwang bei vielen Banken und Sparkassen, ihre Geschäftsmodelle anpassen zu müssen. Um dies möglichst schnell, flexibel und kostensparend bewerkstelligen zu können, entschieden sich einige (vor allem größere) Institute dazu – trotz diverser Vorbehalte hinsichtlich Datensicherheit und Regulatorik – Anwendungen und Projekte in eine sogenannte Private Cloud bei externen Dienstleistern auszulagern.

Es sollte aber nicht bei diesen ersten Gehversuchen bleiben: Mittlerweile verstehen viele Institute die Cloud als zentralen Baustein für Innovationen und Wettbewerbsfähigkeit. Wie die PwC-Studie „Cloud Computing im Bankensektor 2021" zeigt, nutzen aktuell 78 Prozent der deutschen Banken Cloud-Lösungen. Das entspricht einem Anstieg um 25 Prozentpunkte im Vergleich zum Jahr 2018. Gut die Hälfte der Banken, die bislang noch keine Cloud verwenden, planen absehbar eine Umstellung. Bei 73 Prozent aller Banken ist die Cloud-Nutzung bereits fester Bestandteil ihrer Strategie. Darüber hinaus ist auch die Bereitschaft gestiegen, größere Datenpakete in Public Clouds, wobei die Daten im Gegensatz zur Private Cloud auf öffentlichen Servern liegen, hochzuladen.

Bei diesen dominieren wenige große Anbieter den Markt und teilen etwa 60 Prozent des weltweiten Cloud-Computing-Angebots unter sich auf: International betrachtet führt gemäß des aktuellen ti&m-Marktüberblicks Amazon AWS das Feld an, dicht gefolgt von Microsoft Azure, Google Cloud, IBM Cloud und Alibaba Cloud. Auf dem deutschen Markt liegt hingegen Google als alleiniger Partner der Deutschen Bank oder der Sparkassen hoch im Kurs. Aber auch die Commerzbank, Comdirect, ING, J.P. Morgan oder Goldman Sachs vertrauen zumindest teilweise auf die Serverfarmen des Unternehmens aus Mountain View. Sehr beliebt ist aber auch der sogenannte Multi-Cloud-Ansatz, den beispielsweise unter anderem einige genossenschaftliche Institute verfolgen. Bei diesem schließen die Institute mehrere Partnerschaften mit unterschiedlichen Cloud-Anbietern, um die jeweiligen Vorteile für sich ausloten zu können und möglichst flexibel zu sein.

Sicherlich können die Bankhäuser mithilfe dieser Technologien neue Potenziale erschließen. Doch bei allem Enthusiasmus zum Fortschritt darf nicht vergessen werden, dass digitale Entwicklungen in der Bankenwelt auch Risiken mit sich bringen. So mahnt auch die Bundesbank in ihrem Monatsbericht für den Juli zu vermehrter Vorsicht: „Bei der digitalen Transformation darf die Sicherheit nicht aus den Augen verloren werden, zumal Banken immer mehr in den Fokus von professionellen Angreifern rücken."

Und diese Sorge hat durchaus ihre Daseinsberechtigung, denn besonders in den vergangenen Jahren sind die Geldinstitute und auch deren Partner immer wieder in das Visier von Hackern geraten. Diese Bedrohung hat sich während der Corona-Pandemie noch einmal verschärft. So legten Angreifer erst kürzlich beispielsweise die Webdienste des IT-Dienstleisters Fiducia & GAD mit einer den Server überlastenden DDoS-Attacke lahm. Eine andere Hackergruppe namens Revil nahm sich nur wenige Wochen später die US-Informationstechnologiefirma Kaseya mit einem Supply-Chain-Angriff zur Brust. Dieser einzelne Cyberangriff wirkte sich auf etwa 1 300 Unternehmen weltweit aus. Mit 70 Millionen US-Dollar wurde eine Rekordsumme an Lösegeld gefordert.

Auch wenn in beiden eben beschriebenen Fällen entsprechende Maßnahmen und Lösungen

zur Abwehr des Angriffs gefunden werden konnten, wird deutlich, welche verheerenden Folgen beziehungsweise Dominoeffekte Cyberangriffe auslösen können. Nicht auszudenken, welche Tragweite eine erfolgreiche Attacke auf eine Public Cloud haben könnte. Und in Zeiten, wo 14-jährige Schüler Staatscomputer hacken können oder andersherum Staaten – darunter auch Deutschland – Trojaner auf Endgeräten unbemerkt installieren dürfen, um beispielsweise Videokonferenzen mitverfolgen zu können, stellt sich doch schnell die Frage: Ist heutzutage überhaupt noch irgendetwas wirklich sicher?

Um sich als Bank selbst sowie die sensiblen Daten der Kunden schützen zu können, muss das Risikomanagement entsprechend im Vorfeld auf der Hut sein. Doch auch hier entdeckte die Aufsicht schwerwiegende Probleme: Bei mehr als 2000 Inspektionen im Rahmen ihrer bankgeschäftlichen Prüfungen konnte die Bundesbank bei den Kreditinstituten seit dem Jahr 2010 bei fast jeder zweiten Prüfung erhebliche Mängel im Risikomanagement feststellen. Rund 15 Prozent dieser Fälle betrafen IT-Themen. Besonders im Fokus standen hierbei Cyberrisiken mit 17 Prozent sowie die Auslagerung und der Fremdbezug von IT-Dienstleistungen mit sogar 21 Prozent. Es gab zudem erhebliche Störungen beim Identitäts- und Rechtemanagement (13 Prozent), bei IT-Projekten und Anwendungsentwicklungen (13 Prozent), im Notfallmanagement (9 Prozent), IT-Betrieb (5 Prozent) sowie in der IT-Strategie und der IT-Governance mit jeweils 3 Prozent.

Die Institute müssen also peinlich genau darauf achten, dass sie nicht zugunsten von Innovationen und neuartigen Produkten das mühsam aufgebaute Kundenvertrauen, das sie heutzutage noch deutlich von anderen Konkurrenten wie Fintechs abhebt, verspielen. Dafür sollte vielleicht auch nochmal die Auswahl der Dienstleister unter die Lupe genommen werden. Schließlich gelten für die dominanten US-amerikanischen Player in diesem Bereich andere Spielregeln als in Deutschland beziehungsweise innerhalb der EU. So können die ausgelagerten Daten gemäß dem Cloud-Act (Clarifying Lawful Overseas Use of Data Act) vor US-Behörden nicht ausreichend geschützt werden. Denn diese können US-Firmen zwingen, Daten offenzulegen, egal wo diese gespeichert werden. Das heißt, selbst wenn amerikanische Rechenzentren auf europäischem Boden gebaut werden, ist das kein Garant für Sicherheit. Auch deswegen wurde und wird das Cloud-Computing von vielen Experten immer wieder kritisch betrachtet.

Da die Anbieter allerdings selbst ein großes Sicherheitsinteresse hegen und ihre europäischen Kunden sicherlich auch nicht verprellen möchten, haben die Dienstleister angefangen, dieses Risiko durch neue Verschlüsselungstechniken auszuhebeln. Wenn die Banken also Daten selbstständig verschlüsseln und sie die Datenhoheit über diese Schlüssel besitzen, dann bleiben die Daten auch für die US-Behörden vorerst unleserlich. Ob dieser „Trick 17“ nicht selbst ausgehebelt werden kann, bleibt allerdings fraglich.

Besser wäre es, wenn die Politik sich hier für standardisierte Regeln einsetzen würde, die es den Behörden schlichtweg verbietet, Kundendaten einzusehen. Immerhin wird aber bereits kräftig am Cloud-Projekt GAIA-X getüftelt, um sich ein Stück weit von der Abhängigkeit der Anbieter aus dem Ausland lösen zu können. Allerdings befindet sich dieses Projekt immer noch in der Entwicklung. Es gibt zwar erste Standards für die Mitglieder in Bezug auf Themen wie Transparenz, Datenschutz oder Sicherheit, aber am Ende muss so ein System auch mit den bestehenden Wettbewerbern mithalten können und nicht nur Sicherheitsaspekte abdecken.

Bevor das nicht passiert ist, empfiehlt es sich für europäische Banken, nur kleinere Einheiten in die Cloud zu integrieren und zusammen mit dem IT-Dienstleister eine Strategie für die Zusammenarbeit zu erarbeiten. Es muss schließlich nicht alles in die Cloud ausgelagert werden. Um sich des Weiteren gegen digitale Risiken wappnen zu können, reicht laut Bundesbank aber ohnehin die reine Technik nicht aus. Auch die menschliche Komponente, technisch-organisatorische Maßnahmen sowie gut strukturierte und wirksame Prozesse seien entscheidende Erfolgsfaktoren. Auch an dieser Baustelle hat die deutsche Bankenlandschaft noch zu arbeiten!