

DIE ZUKUNFT LIEGT IN DER CLOUD

Das Verlagern von IT-Services in die Cloud ruft die Aufsicht auf den Plan

Technologien wie Cloud-Computing, offene Schnittstellen und Künstliche Intelligenz (KI) eröffnen Finanzdienstleistern völlig neue Möglichkeiten, mit Kunden zu interagieren, Produkte zu gestalten und Prozesse zu steuern. Banken legen bereits das Fundament für diese Zukunft: Rund 80 Prozent der deutschen Banken möchten laut einer PwC-Studie zum Thema „Cloud-Computing im Bankensektor“ zukünftig verstärkt IT-Dienstleistungen über die Cloud nutzen. Auch die Aufsicht adressiert das Thema und begleitet Finanzdienstleister bei deren digitaler Transformation.

Cloud-Technologien sind das Tor zum Banking der Zukunft. Die uneingeschränkte Skalierbarkeit von Rechen- und Speicherressourcen sowie der Zugang zu intelligenten Cloud-Diensten sind Game-Changer in der Finanzindustrie. Das Verlagern von IT-Services in die Cloud ruft die Aufsicht auf den Plan. Für die Deutsche Bundesbank, die Europäische Zentralbank und auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sind Cloud-Computing und -Dienste hoch relevant. Sie führen mit Banken sowie IT- und Cloud-Dienstleistern konstruktive Dialoge, um praktikable Lösungswege für den Einsatz dieser Zukunftstechnologien zu definieren. Gleichzeitig richten sie den Fokus ihrer Prüfungen auf die damit verbundenen IT-Risiken.

Regulatoren im Dialog

Die Rahmenbedingungen für den Einsatz von Cloud-Computing bei deutschen Banken sind im Rundschreiben „Bankaufsichtliche Anforderungen an die IT“ (BAIT) beschrieben. Diese Mindestanforderungen an das Risikomanagement der Banken (MaRisk) gelten auch für Cloud-Dienste, die eine Auslagerung von IT-Dienstleistungen darstellen.

Neben den Regelwerken haben BaFin und Deutsche Bundesbank gemeinsam eine „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ veröffentlicht. Darüber hinaus stehen

sie über das Sonderfachgremium IT zum Thema Cloud/Weiterverlagerung im regelmäßigen Austausch mit den Banken.

Im Fachgremium diskutieren die Teilnehmer konkrete Sachverhalte und Hemmnisse, die sich in der Praxis bei der Umsetzung der Richtlinien ergeben. Die Mitglieder des Sondergremiums haben sich dabei zum Beispiel mit den Anforderungen an die Weiterverlagerung von Cloud-Services befasst. Banken stehen insbesondere bei der Zusammenarbeit mit globalen Cloud-Service-Providern (CSP) vor der Herausforderung, vollständige Transparenz über alle bestehenden Subdienstleistungen zu schaffen. Globale CSPs arbeiten mit einer Vielzahl an Subdienstleistern, machen dies aber gegenüber ihren Kunden nicht ausreichend transparent. In dem Gremium wurde daraufhin ein mehrstufiges Vorgehen erarbeitet: Vorab ist mit dem CSP eine Logik zur Klassifizierung von Dienstleistern zu vereinbaren.

Dienstleister, die für ein Institut als Weiterverlagerung angesehen werden könnten, sind als „potenziell relevante“ Subdienstleister zu klassifizieren. Bei neuen Dienstleistern soll in einem ersten Schritt der CSP die „potenziell relevanten“ Subdienstleistungen identifizieren und dem Institut zur Verfügung stellen. Dieses identifiziert in einem zweiten Schritt die „tatsächlich relevanten“ Subdienstleistungen.

Banken in der Pflicht

Banken müssen sicherstellen, dass ihre IT regulationskonform betrieben wird und Prüfer Transparenz sowie Durchgriffsrechte erhalten. Zudem gelten die gesetzlichen Anforderungen an Datenschutz und Datensicherheit natürlich auch für Cloud-Umgebungen. Neben den klassischen Betriebsumgebungen für den Mainframe benötigen Finanzdienstleister grundsätzlich drei Cloud-Säulen, in denen Daten je nach Leistungsschnitt, Modernisierungsgrad und Schutzbedürfnis sowohl in Private-, Hybrid- oder Public-Cloud-Szenarien verarbeitet werden können: Zum einen eine On-Premise-Cloud-Plattform für den Betrieb ihrer auf Linux- beziehungsweise Windows-Server-basierter Enterprise-IT. Zum anderen für das Modernisieren ihrer IT-Landschaft eine Private-Cloud-Plattform, in der Anwendungen auf Basis von Kubernetes und Containern regulationskonform On-Premise betrieben werden. Darüber hinaus nutzen Banken Public Cloud-Umgebungen von Hyperscalern, wenn sie etwa intelligente KI-basierte Cloud-Dienste nutzen.

Während in den On-Premise betriebenen Cloud-Umgebungen das Einhalten der Anforderungen der Aufsicht zwar aufwändig, aber möglich ist, stellen Hyperscaler-Angebote die Institute regelmäßig vor Herausforderungen. Das zeigt auch der aktuell in dem Sonderfachgremium IT diskutierte Sachverhalt zur Weiterverlagerung von Cloud-Services. Globale CSPs schließen zwar mit einzelnen Instituten Rahmenverträge ab. Je nach genutztem Service des CSPs gelten zusätzliche Nutzungsbedingungen, die die Vereinbarungen des Rahmenvertrags dominieren beziehungsweise einschränken können. Zudem werden die Vielzahl an gültigen Dokumenten,



die in Summe das Vertragswerk ausmachen, durch den CSP häufig einseitig und ohne gesonderte Ankündigung geändert. Institute stehen damit auch seitens der Aufsicht in der Pflicht, das Vertragswerk regelmäßig zu prüfen und Vertragsänderungen hinsichtlich ihrer regulatorischen Relevanz zu bewerten. Denn bei aller Bereitschaft zum Dialog entlässt die Aufsicht Institute nicht aus der Pflicht, ihre Geschäftspartner sorgfältig zu prüfen.

Synergien nutzen

Das Nutzen von Cloud-Diensten von CSPs ist risikobehaftet. Banken müssen dem mit klassischen Methoden der Risikobehandlung begegnen. Sie können Risiken verlagern, reduzieren oder akzeptieren, was heißt, Hyperscaler-Clouds nur für unbedenkliche Daten zu nutzen. Bei allen drei Methoden empfiehlt es sich, auf Synergien zu setzen. Das spart zum einen Kosten und zum anderen bietet es auch gegenüber der Aufsicht Klarheit, wenn bereits geprüfte Best Practices genutzt werden. Die Zusammenarbeit mit auf die Finanzwirtschaft spezialisierten IT-Dienstleistern bietet solche Synergien. Der größte IT-Dienstleister der Landesbanken und IT-Provider zahlreicher anderer Finanzinstitute,

Finanz Informatik Technologie Service (FI-TS), bietet auf Basis einer 3-Säulen-Cloud-Strategie regulationskonforme Cloud-Infrastrukturen für Finanzdienstleister an. Über die Säule „Finance Cloud Public Integration“ hilft der Provider, die Cloud-Risiken der Banken zu verlagern, zu reduzieren beziehungsweise akzeptierte Risiken zu managen. Dazu ergänzt der Provider seine eigenen Prozesse um spezifische Elemente und bezieht sie damit auch auf die CSPs. Konkret: Da CSPs kein bankenspezifisches Risikomanagement anbieten, bindet FI-TS die Hyperscaler-Infrastrukturen an das eigene Risikomanagement an und verarbeitet die Risikoquellen mit regulationsbewährten Methoden. Banken erhalten damit auch für Hyperscaler-Clouds Revisionsberichte, Audit Reportings etc. Gleiches bietet der Providerauch für die regulatorischen Bereiche Interne Revision, Providermanagement und Informationssicherheit an. Darüber hinaus engagiert er sich in Cloud-Gremien wie der Collaborative Cloud Audit Group. Im Verbund mit seinem Gesellschafter Finanz Informatik (FI), dem Digitalisierungspartner der Sparkassen-Finanzgruppe, steht er zudem im regelmäßigen Dialog mit der Aufsicht und deren Organen.

Zahlreiche Banken – darunter einige systemrelevante Institute – verlagern auf diese Weise Aufgaben aus dem Risikomanagement, der Vertragsgestaltung mit CSPs, der Informationssicherheit und der Internen Revision an einen externen Partner. Dieser bündelt die Interessen der Banken, wenn er mit CSPs Rahmenvereinbarungen verhandelt oder im Austausch mit der Aufsicht steht, um praktikable Lösungen zur Einhaltung regulatorischer Vorgaben zu finden. Das schließt auch das Sub-Providermanagement sowie die Exit-Strategien ein.

Weg in die Zukunft

Cloud-Computing ist eine der wesentlichen Technologien für das digitale Banking der Zukunft. Für den Weg in die Cloud hat die Aufsicht den Banken klare Leitplanken gesetzt. Sie schränken die Institute nicht unbedingt ein, machen das Nutzen von Cloud-Technologien und -Diensten aber komplex. Branchenversierte Dienstleister schaffen dabei Synergien und unterstützen dabei, neue Wege effizient zu gehen.

Autor: Dr. Christian Thiel



Dr. Christian Thiel ist seit Januar 2020 in der Geschäftsführung von FI-TS. Er trägt die Verantwortung für Internal Audit, Compliance,

Betriebswirtschaft, Vertrieb, Marketing sowie Architektur- und Produktmanagement

Autor: Klaus Iberle



Klaus Iberle ist seit März 2020 Bereichsleiter Governance, Risk, Compliance bei FI-TS. Neben seinen Stationen in der Wirtschaftsprüfung und

Beratung bei PwC und KPMG hat er auch einige Jahre in der BayernLB gearbeitet.