© Altayb/Getty Images/iStock

Besser für den Notfall gewappnet sein

Deutsche Banken und Sparkassen zieht es in die Cloud. Sie modernisieren ihre Anwendungen, um Banking-Services nach und nach dynamisch zur Verfügung zu stellen. Die Leitplanken setzt dabei die Aufsicht.

Christian Thiel

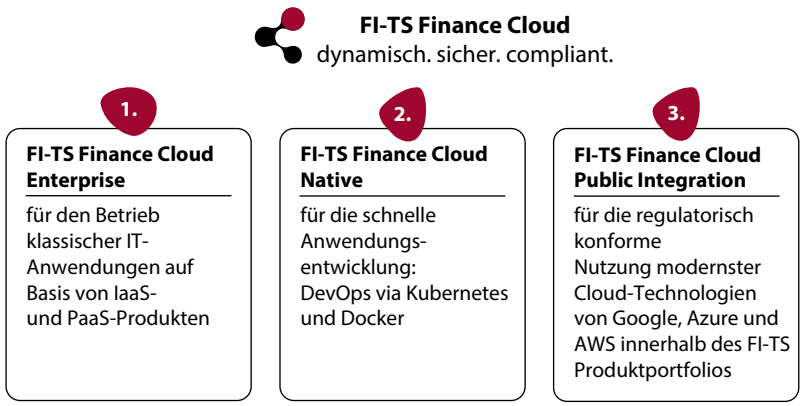
Die Zahlen sprechen für sich: Vier von fünf deutschen Banken möchten laut einer PwC-Studie zum Thema „Cloud Computing im Bankensektor“ künftig verstärkt IT-Dienstleistungen über die Cloud nutzen (siehe Digitaltipp auf Seite 40). Das „New Business“ der scheinbar unbegrenzten Möglichkeiten ruft die Aufsicht auf den Plan. Denn Banking ist ein hochsensibles Geschäft und damit reguliertes Terrain. Deutsche Bundesbank, Europäische Zentralbank (EZB) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) begleiten deutsche Kreditinstitute und deren IT-Dienstleister bei ihrem Weg in die Cloud. Sie führen konstruktive Dialoge, um praktikable Wege für den Einsatz der Cloud-Technologien bei Finanzhäusern zu finden. Ihre Prämisse lautet dabei: Den technologischen Fortschritt unterstützen, aber darauf achten, dass die damit verbundenen IT-Risiken beherrschbar sind. Die Mindestanforderungen an das Risikomanagement der Banken (MaRisk) gelten auch für Cloud-Dienste. Denn letztlich sind sie eine Auslagerung von IT-Dienstleistungen. Die Konkretisierungen dafür sind im Rundschreiben „Bankaufsichtliche Anforderungen an die IT“ (BAIT) beschrieben.

Der regulationskonforme Betrieb von Cloud-Umgebungen erfordert professionelle Strukturen, in denen Daten je nach

Kompakt

- Geldhäuser nutzen verstärkt IT-Dienstleistungen über die Cloud.
- Es muss gewährleistet sein, dass die damit verbundenen IT-Risiken beherrschbar sind.
- Auflagen zum Notfallmanagement gibt es in den Bankaufsichtlichen Anforderungen an die IT (BAIT).

Regulationskonforme Cloud-Services basieren auf einer Drei-Säulen-Cloud-Strategie



Quelle: FI-TS

Leistungsschnitt, Modernisierungsgrad und Schutzbedürfnis in Private-, Hybrid- und Public-Cloud-Szenarien verarbeitet werden können. Neben klassischen Betriebsumgebungen für den Mainframe bestehen diese aus drei Cloud-Säulen:

- Auf einer On-Premise-Cloud-Plattform erfolgt der Betrieb der auf Linux- beziehungsweise Windows-Servern-basierten Enterprise-IT.
- Eine Private-Cloud-Plattform ermöglicht das Modernisieren der IT-Landschaft, in der Anwendungen auf Basis von Kubernetes und Containern betrieben werden. Diese Säule setzt ebenfalls auf einen selbstständigen On-Premise-Betrieb und erfüllt damit zweifelsfrei hohe regulatorische Ansprüche.
- Neben diesen beiden essenziellen Säulen können Geldhäuser auch Public-Cloud-Umgebungen von Hyperscalern nutzen. Dabei hat das Institut sicherzustellen, dass dort nur Daten verarbeitet werden, deren Verarbeitung in Public Clouds unkritisch ist.

Cloud-Strategie basiert auf drei Säulen

Als IT-Dienstleister von Landesbanken sowie IT-Provider zahlreicher anderer Finanzinstitute hat Finanz Informatik Technologie Service (FI-TS) ihre regulationskonformen Cloud-Services auf Basis einer Drei-Säulen-Cloud-Strategie organisiert (siehe Grafik oben). Die ersten beiden Säulen bilden eine Community-Cloud für Banken und Versicherer, in der unternehmenswichtige und notfallrelevante Geschäftsprozesse betrieben werden. Die erste Säule, die Finance Cloud Enterprise, ermöglicht Banken einen regulatorisch konformen Betrieb von Bestandssystemen. FI-TS Finance Cloud Native, die zweite Säule der Community-Cloud, ist eine Plattform für modernisierte Anwendungen. Sie unterstützt moderne Microservice-Architekturen, für die der Provider in eigenen Rechenzentren in Deutschland Kubernetes als Cloud-Service zur Verfügung stellt.

Wie weitreichend die Anforderungen der Aufsicht die Organisation und das Management der Community-Cloud für Banken und Versicherungsgesellschaften bestimmen, zeigt sich am Beispiel des Notfallmanagements. Die Aufsicht fordert in den BAIT, dass Institute Ziele zum Notfallmanagement definieren und daraus Notfallmanagementprozesse ableiten sowie für Notfälle in zeitkritischen Aktivitäten und Prozessen Vorsorge treffen müssen. Die im entsprechenden Notfallkonzept festgelegten Maßnahmen sollen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren.

Um diese Anforderungen zu erfüllen, betreibt FI-TS alle Instanzen der Community-Cloud in räumlich getrennten Rechenzentrumspaaren und organisiert den Business Continuity-Prozess entsprechend den Empfehlungen der ISO 22301. Dabei berücksichtigt der Provider auch die Sicherheitsstandards BSI 100-4 des Bundesamts für Sicherheit in der Informationstechnik (BSI).

In beiden Säulen der Community-Cloud sind im jeweiligen technologischen Umfeld Notfall-Lösungen implementiert, mit denen unterschiedlichste Wiederherstellzeiten von Geschäftsprozessen sichergestellt werden. Gemeinsam mit den Banken identifiziert der Provider die notfallkritischen Geschäftsprozesse und legt entsprechend den technischen Möglichkeiten und wirtschaftlichen Interessen der Kunden die jeweils angemessenen Wiederherstellzeiten fest. Das reicht von der Gewährleistung einer quasi unterbrechungsfreien Bereitstellung hoch kritischer Geschäftsprozesse wie etwa dem

Betrieb von Onlinebanking-Anwendungen bis hin zu Wiederherstellzeiten innerhalb mehrerer Stunden. Entsprechend dieser Definition implementiert der Provider die jeweiligen Geschäftsprozesse in der relevanten Cloud-Säule und bindet sie in die Notfallmechanismen ein.

Ein eigenes Business-Continuity-Management-Team kümmert sich beim Provider um die organisatorischen Rahmenbedingungen, innerhalb derer die Notfallprozesse aufgesetzt, eingehalten und deren Einhaltung dokumentiert werden. Das Team organisiert unterjährig regelmäßige Notfalltests, mit denen die Absicherung insbesondere auch neuer Services und Geschäftsprozesse überprüft wird. Einmal pro Jahr findet mit jedem Kunden eine Notfallübung statt, bei der Ausfälle unterschiedlichster Geschäftsprozesse und das Einhalten der zugesagten Service-Level verprobt werden.

Alle zwei bis vier Jahre wird der komplette Ausfall eines Rechenzentrumsstandorts simuliert. Von diesem Großereignis sind stets mehrere Kunden betroffen. Geübt wird, wie das gepaarte Rechenzentrum nahtlos den Betrieb des betroffenen Standorts übernimmt. Alle Tests und deren Ergebnisse werden analysiert und dokumentiert. Identifizierte Risikofaktoren werden behoben und das Zusammenspiel aller Komponenten fortwährend optimiert. Die Dokumentationen der Tests und deren Ergebnisse dienen der Aufsicht als Nachweis, dass die entsprechenden regulatorischen Anforderungen durch die beteiligten Kreditinstitute eingehalten und alle Vorgaben erfüllt werden.

Den Anforderungen der Aufsicht an ein Notfallmanagement wird so Rechnung getragen. Vergleichbare Anforderungen stellen die MaRisk und die BAIT an viele weitere Gebiete des Betriebs von Cloud-Umgebungen. Dabei sind die Anforderungen nicht in Stein gemeißelt, sondern entwickeln sich genauso dynamisch, wie sich die Cloud-Technologien weiterentwickeln. Deshalb ist es essenziell, mit der Aufsicht im Dialog zu stehen. Nur so kann künftig Relevantes frühzeitig antizipiert und auch über die Grenzen des praktisch Umsetzbaren gesprochen werden. Der Dialog gewährleistet, dass Banken und Sparkassen dynamisch, sicher und compliant von den Vorteilen des Cloud Computings profitieren können. ■

© FI-TS

Autor

Christian Thiel

ist Geschäftsführer von Finanz Informatik Technologie Service (FI-TS) und Experte für aufsichtsrechtliche Anforderungen an die IT der Banken- und Versicherungsbranche.

Springer Professional

Cloud Computing

Angelika Breinich-Schilly: Finanzindustrie gibt bei Cloud-Technologien Gas, Wiesbaden 2022
https://sn.pub/8DMQJZ

Sylvia Meier: Cloudbasierte Plattformen machen Finance zukunftsfähig, Wiesbaden 2022
https://sn.pub/dvySzm

Alexander Zachow: Banken benötigen flexible und skalierbare Lösungen,
in: Bankmagazin 4/2023
https://sn.pub/aWDHMo

Anja Kühner: Das Banking in Scheiben schneiden,
in: Bankmagazin 4/2023
https://sn.pub/0uZZe3

Christian Glaser: IT-Regulatorik und -Sicherheit als Basis der Digitalisierung, in: Digitale Transformation im Bankenumfeld, Wiesbaden 2022
https://sn.pub/goK1aN

Weitere Digitaltipps

Links

- Aktuelle Fassung der Bankaufsichtlichen Anforderungen an die IT (BAIT): https://sn.pub/sFQyGD

Studien

- PwC-Studie „Cloud Computing im Bankensektor 2021“: https://sn.pub/eDLdZa