Risikomanagement im As-a-Service-Zeitalter

Das Betriebsmodell der Zukunft: Warum Banken und ihre Dienstleister eine neue Compliance-Praxis brauchen, um die Chancen und Risiken von As-a-Service-Angeboten auszubalancieren.

Autor:
Frank Bastian,
ISG Information Services Group

Compliance neu denken, um Risiken von As-a-Service-Angeboten richtig ausloten zu können

Der Kostendruck in der Kreditwirtschaft wächst weiter. Während ein Ende der aktuellen Ertragskrise kaum absehbar ist, erweisen sich As-a-Service-Dienste als starkes Mittel, um die Sparziele der Unternehmen auch zukünftig noch erfüllen zu können. Dies setzt jedoch voraus, dass Banken gezielter Risiken adressieren und nicht nur pauschal Vertrags-/Dienstleisterrisiken verwalten. Zudem müssen sie stärker darauf dringen, dass ihre Dienstleister das nötige Geschäfts- und Prozesswissen vorhalten.

Kein Zweifel: As-a-Service ist das Betriebsmodell der Zukunft, um Banktechnologien marktgerecht bereitzustellen und flexibel einzusetzen. Nutzungsabhängig abrechenbare Cloud-Dienste adressieren Front-, Middle- und Back-Office-Prozesse inzwischen gleichermaßen. Ziel ist der Bau durchgängiger End-to-End-Lösungen, die sich den Bedürfnissen der Bankkunden entsprechend immer wieder neu ausrichten lassen. So weit, so gut. Doch wer sich, wie die Bankenwelt, aus einer extrem proprietären IT-Welt herausentwickelt und somit aktuell nicht über die erforderlichen Mittel verfügt, kann die Transformation nur schrittweise angehen. Passende As-a-Service-Modelle lassen sich daher nur evolutionär entwickeln.

Vorzugsweise beginnt man dort, wo Innovationen besonders schnell einen Mehrwert bringen. So zum Beispiel, wenn es darum geht, die Kreditwürdigkeit von Darlehensinteressenten genauer zu beurteilen. Hier gibt es bereits jetzt clever gemachte FinTech-Angebote, die Schufa-Auskünfte mit Sekundärdaten aus dem Internet anreichern und damit wesentlich aussagekräftiger machen. Ein solcher Dienst wirkt vertikal in die Prozessmatrix des Kreditgeschäfts hinein. Für sich genommen ist ein solches As-a-Service-Rating also erst einmal ein spezifischer Teilschritt. Gleichwohl vermag er es, die Performance des Gesamtprozesses – hier Kreditvergabe – signifikant zu erhöhen.

Schaut man auf die Verbreitung von As-a-Service-Lösungen im deutschsprachigen Bankenraum, so haben vertikale Teillösungen derzeit die größten Marktanteile. Ungeachtet dessen steigt die Zahl der Unternehmen, die sich an Komplettlösungen heranwagen. Sie übernehmen, um im oben genannten Prozessbeispiel zu bleiben, die komplette Abwicklung des Ratenkredits. Weiteren Schub erhält die Verbreitung von As-a-Service-Modellen zum Teil auch durch regulatorische Veränderungen. So zum Beispiel durch die EU-Richtlinie PSD2 (Payment Service Directive 2), dank derer die Marktöffnung der Zahlungsdienste immer mehr Fahrt aufnimmt.

Top-Hindernis: Defensiver Umgang mit Regulatorik

Da die Umsetzung dieser Richtlinie alte Gewissheiten massiv in Frage stellt, eignet sich das PSD2-Umfeld gut, um näher auf diejenigen Herausforderungen zu schauen, mit denen es die traditionsreiche Banken- und Sparkassenlandschaft im DACH-Raum in besonderer Weise zu tun hat. Denn Top-Hindernis Nummer eins ist der eher konservative Umgang mit regulatorischen Vorgaben und damit verbunden die eingeschränkte Bereitschaft, unternehmerische Risiken mitunter auch mit ungewohnten Mitteln einzugehen. Doch ist diese Zurückhaltung keineswegs nur das Ergebnis der Unternehmenskultur in den Kredithäusern. Mindestens genauso stark resultiert sie aus den Erwartungen an die Zusammenarbeit mit IT-Dienstleistern. Letztere nehmen allzu oft die Rolle des Umsetzers ein. Schließlich konzentriert sich das klassische Anspruchsdenken der Bankenwelt darauf, dass die Infrastruktur, auf der ihre Dienste aufsetzen, als Ganzes compliant sein soll. Und zwar sowohl in technologischer Hinsicht, etwa bei Fragen der Kryptografie, als auch mit Blick auf die Einhaltung organisatorischer Vorgaben, wenn es zum Beispiel um die Anwendung des Weisungsrechts oder die Durchführung von Audits geht.

Wer die Vorzüge der As-a-Service-Welt erschließen will, sollte den Elefanten allerdings deutlich kleiner machen: Banken, wie auch ihre Provider, sollten dann nicht mehr länger das Data Center als Ganzes betrachten, sondern die spezifischen Geschäftsvorfälle, die von einem Cloud-Dienst berührt werden. Somit geht es zuallererst um konzeptionelle, prozessbezogene Fragen, welche das tatsächliche Ausmaß der As-a-Service-Risiken klären und erst dann im zweiten Schritt um den Zuschnitt der Methoden, mit denen das angestrebte Zielniveau bei Datenschutz und Datensicherheit erreicht werden kann.

Wie man die Kritikalität der Geschäftsvorfälle klärt

Aufschluss über die tatsächlichen Compliance-Risiken einer neuen As-a-Service-Lösung bringen sogenannte Data Playbooks. Diese stellen vor allem den Use Case und die Datenstrukturen des zu bauenden As-a-Service-Modells dar. Beispiel: Nehmen wir an, eine Bank fasst den Plan, die Gesamtheit der bei ihr auflaufenden Geldkartendaten einem Analyse-Dienst zur Verfügung zu stellen, der ein präziseres Bild über das Kaufverhalten der Bankkunden ermitteln will.

Um datenschutzkonform vorzugehen, müssen das Geldinstitut respektive sein(e) IT-Dienstleister die Kundendaten so vorfiltern und kategorisieren (etwa nach Altersgruppen), dass im Rahmen der Datenanalyse keinerlei Rückschlüsse auf einzelne Kunden mehr möglich sind. Die mit der Aufbereitung, Bereitstellung und Analyse der Kundendaten einhergehenden Systembeziehungen, Datenstrukturen und Informationszustände beschreibt das Data Playbook. Eine solche Dokumentation sauber aufzusetzen, aktuell zu halten und auf die konkret ins Auge gefassten Geschäftsvorfälle zu beziehen, ist essenziell, um als As-a-Service-Provider in einem hochregulierten Markt wie dem Finanzsektor mitdenken und dann vor allem auch mitdiskutieren zu können. Dass Dienstleister die Technik beherrschen, um As-a-Service-Lösungen zu betreiben, wird hierbei vorausgesetzt. Die Differenzierung im Markt und der Vorteil für den Kunden werden aber erst durch das notwendige Geschäfts- und Beratungswissen real.

Beratungswissen als Disruptionsschutz

Indem sie ihren technologischen Sachverstand mit handfestem Know-how zu den regulatorischen Risiken der Geschäftsvorfälle verbinden, schließen die Provider dann eine echte Bedarfslücke. Denn erst dies ermöglicht eine Argumentation mit den Risiko-, Security- und IT-Managern in den Geldhäusern auf Augenhöhe. Vor diesem Hintergrund bieten Data Playbooks und die in ihnen beschriebenen Use Cases eine ungeahnt aussagekräftige Gesprächsgrundlage, anhand derer sich Risiken präzise aufzeigen lassen, um sie dann nach einer positiven Abwägung mit dem erreichbaren Nutzen kontrolliert eingehen zu können.

Beispiel: Angenommen, das Aufsetzen eines neuen Cloud-Dienstes führt tatsächlich dazu, dass das Geldinstitut die Vorgaben des Weisungsrechts nicht mehr vollständig durchsetzen kann. Diese Annahme betrifft ein Szenario, an das sich die Verantwortlichen in den Banken mehr und mehr gewöhnen müssen. Vor allem dann, wenn sie mit weltweit operierenden Dienstleistern wie AWS, Azure oder Google ins Geschäft kommen wollen. Erst über den Use Case wird dann klar ersichtlich, welche Kritikalität die herausgegebenen Daten am Ende des Tages denn tatsächlich haben.

Mit diesem Informationsstand kann der Vorstand sachlich abwägen, wie die Reaktion der Aufsichtsbehörden ausfallen wird und inwiefern der Nutzen der in Aussicht gestellten As-a-Service-Lösung es nahelegt, diese Risiken bewusst einzugehen. Zumal es neben den Compliance-Risiken eine stetig steigende Zahl weiterer Risiken ins Kalkül zu nehmen gilt.

Allen voran die Gefahr, durch eine zu große Cloud-Zurückhaltung gegenüber globalen Mitbewerbern Marktanteile zu verlieren. Wer stattdessen die disruptive Welle besser gleich selbst reiten will, bekommt mit den Data Playbooks ein flexibles Mittel an die Hand, um As-a-Service-Lösungen nicht nur ertragssteigernd, sondern auch sicher einzusetzen.