Cloud for the financial industry

Positionspapier des FinTechRats

21. März 2019

Inhalt

Zielsetzung

Der Finanzmarkt entwickelt sich immer mehr zu einem Ökosystem, in dem die Leistungserstellung nicht durch einzelne Institute sondern durch Kooperation zwischen verschiedenen Marktteilnehmern entlang der Wertschöpfungskette erfolgt. Dies ändert die Anforderungen an eine zeitgemäße Regulatorik hinsichtlich der Erfassung der Marktteilnehmer, der Transparenz über Schnittstellen, Verantwortungen und Risikoentwicklungen sowie der Reaktionsmöglichkeiten bei Fehlentwicklungen.

Effiziente Informationstechnologie, insbesondere Cloud-Technologie, wird dabei als ein Schlüsselelement zukünftiger Leistungsfähigkeit angesehen. So gaben in einer IDG-Studie aus dem Jahr 2018 73% der befragten US-Unternehmen an, bereits wichtige Teile ihrer technischen Infrastruktur an externe Cloud-Dienstleister ausgelagert zu haben. 4 von 5 der Unternehmen, die dies noch nicht taten, planten entsprechende Schritte für die nächsten 18 Monate. Auch wenn Europa in der Entwicklung noch hinterherläuft, sind vergleichbare Tendenzen zu beobachten und im Sinne der Wettbewerbsfähigkeit und einer nachhaltig leistungsfähigen Infrastruktur auch notwendig. Es geht nicht mehr um das „ob", sondern um das „wie" und „wann". Dabei ist im Koalitionsvertrag der Bundesregierung das klare Ziele definiert, Deutschland zum führenden Standort im Kontext der Digitalisierung der Finanzdienstleistungsindustrie zu entwickeln ("Wir werden uns für attraktive Rahmenbedingungen am Finanzplatz Deutschland einsetzen und die digitale Infrastruktur für die Finanzmärkte weiter stärken."). In diesem Positionspapier sollen Lösungsansätze dargestellt werden, um Cloud-Lösungen als Kernelement digitaler Infrastruktur in Deutschland flächendeckend verwenden zu können. Vorab soll aufgezeigt werden, was Gründe für den heutigen Status quo sind und warum Anpassungsbedarf bei allen Marktteilnehmern, dem Gesetzgeber sowie dem Regulator dringend angeraten ist.

Ziel ist es, eine Lösung zu präsentieren, die bei ganzheitlicher Betrachtung den volkswirtschaftlichen Nutzen maximiert und dabei gleichzeitig allen Betroffenen die bestmögliche Wahrung ihrer Interessen ermöglicht.

- Die *Kunden* wünschen Zugang zu modernen Technologien, die einen hohen Nutzen und eine möglichst gute User Experience versprechen. Typische Kriterien sind dabei Verfügbarkeit, Individualisierbarkeit, konkrete Relevanz, Kosten und Convenience. Diese Kundenwünsche sind wesentliche Treiber der Entwicklung zu einem Ökosystem, in dem Spezialisten für einzelne Teile der Wertschöpfung den Kundennutzen in Summe maximieren. Gleichzeitig haben Kunden höchste Ansprüche an Datenschutz und Sicherheit.
- Der *Gesetzgeber* hat den Anspruch, den Finanzmarkt weiterhin sicher und effizient zu gestalten und den Regulator mit entsprechenden Kompetenzen auszustatten.
- Der *Regulator* muss den Finanzmarkt, bestehend aus den Instituten sowie den Zulieferern und weiteren an der Wertschöpfungskette Beteiligten, effizient und effektiv überwachen können. Die dazu notwendigen Anpassungen an neue Anforderungen sind ebenfalls im Koalitionsvertrag reflektiert ("Wir wollen die Fähigkeiten der

Finanzaufsicht im Bereich Digitalisierung und IT-Sicherheit stärken und auch die Zusammenarbeit mit allen zuständigen Aufsichts- und Sicherheitsbehörden intensivieren.")

- Die *Institute* wünschen sich einen praktikablen Umgang mit Auslagerungen, der die Wettbewerbsfähigkeit unter Nutzung der Vorteile eines leistungsstarken Ökosystems ermöglicht. Der Begriff der Auslagerung i. S. d. KWG stammt aus einer Zeit, in der das Auslagerungswesen anders als heute geprägt war. Die grundsätzlich guten Ansätze sind auf heutige Auslagerungssachverhalte praktisch nicht anwendbar. Des Weiteren führte die bisherige Anwendung in der Praxis zu so individuellen Ausgestaltungen, dass sich nur noch wenige gemeinsame Schnittmengen finden lassen, die ein effizientes Vorgehen für alle Marktteilnehmer ermöglichen würden.
- Die *Cloud-Service-Provider (CSP)* wollen die wachsende Nachfrage aus dem Finanzmarkt bedienen. Die angebotenen Datenschutz- und Sicherheitsstandards sind sehr hoch, da es sich um das „Produkt" von CSP handelt, effiziente und sichere IT bereit zu stellen. Die Strukturen orientieren sich an anerkannten Standards, die typischerweise selbst den Anforderungen an „kritische Infrastrukturen" nach den Maßgaben des BSI genügen.

Zum einheitlichen Verständnis wird im Rahmen dieses Papiers auf die Cloud-Definition des NIST (National Institute of Standards and Technology) abgestellt: „Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Des Weiteren sind die unterschiedlichen möglichen Servicemodelle zu unterscheiden. Auch wenn weitere Zwischenmodelle (bspw. Plattform as a Service) möglich sind, soll im Sinne der klaren Differenzierung insbesondere zwischen den beiden wesentlichen Modellen Infrastructure as a Service (IaaS) und Software as a Service (SaaS) unterschieden werden:

Infrastructure as a Service (IaaS)

Als Infrastruktur werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Kunde kauft oder mietet diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Kunde z.B. Rechenleistung, Arbeitsspeicher und Datenspeicher auch kurzfristig anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen. Entsprechend hat der Kunde auch die volle Kontrolle vom Betriebssystem aufwärts.

Software as a Service (SaaS)

Aufbauend auf der Infrastruktur verwaltet der Service Provider sämtliche Anwendungen, die sich auf der bereitgestellten Cloud-Plattform befinden. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung,

oder Textverarbeitung, aber auch wesentliche Finanzdienstleistungen wie Portfolio Management oder Kreditprozesse genannt. Ein wichtiger Unterschied im Vergleich zu IaaS ist, dass bei SaaS der Cloud-Anwender nur wenige oder gar keine Konfigurationen selber bestimmen und somit verantworten kann.

Historische Entwicklung

In der Finanzindustrie existiert heute ein hoher regulatorischer Standard, der sich historisch entwickelt hat. Kern der gesamten Organisationsstruktur sind die „Leitgesetze“, u. a. das KWG, das KAGB, das VAG sowie das WpHG. Die Grundzüge für das Risikomanagement in den Instituten wurden bereits 1995 durch die „Mindestanforderungen an das Handelsgeschäft“ (MaH), die „Mindestanforderungen an die Interne Revision“ (MaIR, 2000) und die „Mindestanforderungen an das Kreditgeschäft“ (MaK, 2002) formalisiert, die seit 2005 in den „Mindestanforderungen an das Risikomanagement“ (MaRisk) zusammengefasst sind und heute bereits in der fünften Überarbeitung / Novelle vorliegen. Ergänzend gibt es weitere Konkretisierungen wie die MaComp[1], oder die BAIT[2] etc.

Maßgeblich basieren diese Regelungen auf der „prinzipienorientierten Regulierung“ sowie der „doppelten Proportionalität“. Bei der prinzipienorientierten Regulierung legt der Gesetzgeber bzw. der Regulator in seinen Ausführungen Prinzipien fest, die dann von den Instituten auf ihr jeweiliges Geschäftsmodell angepasst auszugestalten sind. Dieser Ansatz ermöglicht es den Instituten, in einer eigenen Analyse den Instituts-individuellen Risikogehalt zu bewerten und die Prozesse sowie die enthaltenen oder darauf aufbauenden Kontrollen angemessen zu gestalten. Die Einstufungen, Ergebnisse, Kontrollen sowie deren Angemessenheit werden dann durch die jeweiligen internen und externen Kontrolleinheiten (Compliance, Revision, Wirtschaftsprüfer und die Aufsicht) geprüft. In der Ausgestaltung von IT sowie den dazugehörigen Kontrollen hat sich im Lauf der vergangenen Jahre gezeigt, dass IT essentielle Grundlage eines jeden Instituts ist. Dies haben nahezu alle Institute erkannt, wie an den zahlreichen Digitalstrategien, CDOs sowie den zunehmenden IT-Kosten zu erkennen ist.

Der Regulator hat mit verschieden Maßnahmen und Konkretisierungen (u.a. BAIT, IT-Kompetenz in der Geschäftsleitung) den zunehmenden Stellenwert der IT auch aus aufsichtsrechtlicher Perspektive klargestellt.

Es gibt heute faktisch keine Prozesse mehr, bei denen nicht an irgendeiner Stelle IT notwendig ist. Dies entspricht der allgemeinen volkswirtschaftlichen Entwicklung und ist heute

[1] MaComp: Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzpflichten

[2] BAIT: Bankaufsichtlichen Anforderungen an die IT; sinngemäß auch VAIT, 2018

selbstverständlich. Technologischer Fortschritt ist die Grundlage für effiziente Prozesse, sowohl institutsintern als auch auf Seiten des Regulators. Er ist somit wünschenswert.

Die IT erfüllt hierbei auf keinen Fall eigene Zwecke, sondern zwingende Anforderungen, um internen sowie marktwirtschaftlichen Effizienzkriterien, Kundenwünschen und nicht zuletzt auch aufsichtsrechtlichen Anforderungen, z. B. im Meldewesen, nachzukommen.

Zusammenfassend lässt sich festhalten, dass die MaRisk, bzw. die Vorläufer, in einer Zeit entstanden sind, in der nur wenige Prozesse ausgelagert wurden und diese zumeist klassischer finanzwirtschaftlicher Natur waren. In den letzten Jahren haben sich aber Art und Umfang von Auslagerungen deutlich gewandelt, ohne dass die regulatorischen Rahmenbedingungen im gleichen Maße weiterentwickelt wurden.

Aktuelle Herausforderungen

Durch die zuvor genannten Entwicklungen hat sich eine Organisations- und Prüfungspraxis etabliert, die auf finanzwirtschaftliche Prozesse anwendbar sein mag. Diese ist jedoch nur für das jeweilige Institut logisch und konsistent und regelmäßig nicht übertragbar. Ausgehend von einer neuen oder geänderten Regulierung[3] wird die Regulierung durch die operativen Einheiten implementiert und durch die Kontrolleinheiten plausibilisiert und geprüft. Ab diesem Zeitpunkt gibt es zwar einen Austausch unter den Häusern wie z. B. durch Branchen- oder Prüfverbände, allerdings ist es üblich, dass jedes Haus seine eigene Sicht auf den jeweiligen Sachverhalt hat. Der weitere Pfad, der sich in einem Institut entwickelt, ist also abweichend von dem Pfad eines anderen Instituts. Bei unterschiedlichen Risikoprofilen der finanzwirtschaftlichen Prozesse entspricht dies auch durchaus dem regulatorisch Gewollten. Bei vergleichbaren Risikoprofilen erschwert es jedoch die risikobasierte Vergleichbarkeit für den Regulator über Institute hinweg. Bei der Ausgestaltung von kritischer Infrastruktur für die gesamte Branche bzw. sogar branchenübergreifender Infrastruktur wie IaaS, wird die bestehende Praxis zum substantiellen Hindernis.

Ein alternativer Ansatz lässt sich am Beispiel der Energieversorgung einer Bank darstellen. Von den Instituten erwartet der Regulator zu Recht, dass sie Maßnahmen vorhalten, die im Falle eines Ausfalls der Stromversorgung für kritische Geschäftsprozesse die Handlungsfähigkeit bewahren. Dies beinhaltet Maßnahmen wie die Definition der kritischen Prozesse sowie das Vorhalten von angemessenen Notfallplänen inklusive Notfallmaßnahmen. Kurzfristig orientiert ist dies z.B. das Vorhalten von Notstromaggregaten. Mittel- bis langfristig gehört beispielsweise das Bereithalten von Ausweichbüros oder die Konzeption von Datenmigrationsplänen dazu. Niemand – weder Wirtschaftsprüfer noch Regulator – erwartet jedoch, dass ein Institut seine internen Kontrollen auf den Energieerzeuger ausweitet. Warum auch? Erstens unterliegt dieser einer gesonderten

[3] Hier zusammenfassend für Gesetz, Direktive, Rundschreiben, etc.

ganzheitlichen, ebenfalls staatlichen Regulierung und zweitens hat eine Bank keine Expertise in der Steuerung und Überwachung von Energiedienstleistern.

Lösungsansatz

Die prinzipienorientierte Ausgestaltung der MaRisk ist grundsätzlich richtig und angemessen. Sie ist zurecht ein fundamentaler Faktor des internationalen Aufsichtsrechts. Jedoch ist eine Weiterentwicklung notwendig, um den Ansprüchen eines leistungsfähigen Ökosystems gerecht zu werden.

So wie der Energiesektor ebenfalls durch Dritte geprüft wird, bzw. im Rahmen des BSI-Gesetzes im Kontext der kritischen Infrastrukturen (UPKRITIS) Nachweise erbringen muss, auf die sich Kunden berufen und verlassen können, bietet sich an, auch für IaaS als branchenübergreifende Infrastruktur eine entsprechende Regulierung und branchenübergreifende Kontrolle zu etablieren. Analog der Energieversorgung könnten Finanzinstitute in ihren eigenen Maßnahmen dann darauf aufsetzen, inkl. der Definition von Backup- und Migrationsplänen, aber ohne die Notwendigkeit eigener Audits des jeweils genutzten IaaS-Providers.

Standards wie der C5 des BSI bieten bereits die Grundlage für eine entsprechende Regulierung von IaaS. Zielsetzung sollte sein:

a) Ein durchgehend hohes technologisches Niveau basierend auf aktueller Hardware und state-of-the-art Prozessen;
b) Etablierung und kontinuierlicher Erhalt des Sicherheitsniveau auf einem sehr hohen Level;
c) Schnelle Reaktionsmöglichkeiten im Falle von technischen oder sicherheitsrelevanten Vorfällen;
d) Volle Skalierbarkeit (auf- und abwärts);
e) Vereinfachte Exit- und Übergangs-Strategien;
f) Stärkung des Wettbewerbs um Innovationen und attraktive Kostenstrukturen zu fördern.

Für den Finanzsektor ist davon auszugehen, dass die genannten Rahmenbedingungen und gut gestaltete Regulierung zudem Konzentrationsrisiken minimieren, indem sich bspw. neue Wettbewerber auf Basis des Equal Playing Fields etablieren und aufgrund der einfacheren Wechselmöglichkeiten Marktanteile gewinnen können.

Im Unterschied zu IaaS ist die Regulierung für SaaS branchenspezifisch auszurichten, da die Kontrolle und Ausgestaltung der Anwendungen durch den SaaS-Anbieter erfolgt. Insbesondere bei finanzwirtschaftlichen, fachfunktionalen Anwendungen wie Portfolio Management oder Kreditprozessen ist auch das Erfordernis eigener KWG-Lizenzen entsprechender SaaS-Anbieter denkbar, um die Konsistenz zwischen tatsächlicher und regulatorischer Verantwortung sicherzustellen. Diese Konsistenz bildet die Grundlage für

Nutzer und Anbieter skalierbar und effizient zusammenzuarbeiten und sichert zugleich die durchgehenden Prüf- und Kontrollrechte der Aufsicht. Klarstellend sei zudem erwähnt, dass auch vom Anspruch an Prüf- und Kontrollrechten für Institute an dieser Stelle nicht abgewichen wird – so wie jeder verantwortungsvolle Kaufmann diese immer in Verträgen verankern wird. Allerdings soll es keine – gesetzliche oder durch Prüfungspraxis manifestierte – Pflicht zu eigenen Prüfungshandlungen durch ein auslagerndes Institut ohne entsprechende Indizien für eine Handlungsnotwendigkeit geben.

Wir sehen in dem genannten Vorgehen sowohl die Möglichkeit, den Instituten den Weg in die Cloud zu ermöglichen, als auch die Möglichkeit für neue CSP, sich einen Markteintritt zu verschaffen. Dies wird auch dazu führen, dass die Oligopolstellung der wenigen großen (zumeist amerikanischen) CSP durch europäische Anbieter hinterfragt wird. Auch neue Geschäftsmodelle, z.B. „regulatorische Schirme“ durch entsprechende Spezialanbieter für SaaS sind denkbar. In Summe entsteht ein effizienterer Markt, der Innovationen und Leistungsfähigkeit fördert und zugleich Risiken reduziert, indem bspw. Finanzinstitute tatsächliche Exit-Möglichkeiten erhalten. Diese sind heute in der Finanzindustrie mit hohen Aufwänden verbunden und oftmals nur auf dem Papier existent.

Die Stärkung der Leistungsfähigkeit des Banken-Ökosystems ist für Kunden elementar. Dies lässt sich gut mit einer schließenden Analogie zeigen: Der internationale Welthandel wurde durch die Einführung des „Standard Containers“ erfolgreich skalierbar gestaltet. Dabei wird ein Container regelmäßig auf seine Stabilität und Verwendbarkeit geprüft und bestätigt. Für den Inhalt eines Containers ist jedoch nur der Verwender verantwortlich. Der Transporteur behandelt den Container nach dessen Vorgaben und hat keinen Einfluss auf den Inhalt. Eine solche Erfolgsstory ist auch im Bereich Cloud absehbar – aber nur bei entsprechender Ausgestaltung der regulatorischen Rahmenbedingungen für den deutschen und europäischen Finanzsektor. Deutschland sollte daher Vorreiter sein, die eigene Gesetzgebung entsprechend ausgestalten und diese zugleich auch auf Europäischer Ebene forcieren.