Cloud-Transformation unter regulatorischen Rahmenbedingungen

Worauf Institute achten sollten

Dass Leasing-Unternehmen den Schritt in die Cloud wagen, scheint mit Blick auf die Entwicklung moderner Technologien nur konsequent zu sein. Aber auch wenn die Cloud-Nutzung viele Vorteile verspricht, sollten Unternehmen die Chancen und Risiken dieser Entscheidung sorgfältig abwägen. Dafür bietet sich ein strukturierter Strategieprozess an. Ist die Entscheidung für die Cloud gefallen, warten umfangreiche regulatorische und institutsindividuelle Anforderungen. Die Autoren wissen, was das alles umfasst und geben Tipps für die praktische Umsetzung. (Red.)

Die Nutzung von Cloud-Technologien verspricht für Leasing-Institute viele Vorteile. IT-Services können schneller bereitgestellt und bedarfsgerecht skaliert werden. Das spart nicht nur Kosten, sondern unterstützt die Geschäftstätigkeit der Institute durch hochverfügbare, digitale Geschäftsprozesse. Vor einigen Jahren war die Nutzung von Cloud-Technologien in der Finanzbranche allerdings beinahe undenkbar. Zu groß war die Unsicherheit im Hinblick auf die Erfüllung regulatorischer Anforderungen und die Angst vor neuen Cyberrisiken. Inzwischen hat sich die Sichtweise radikal geändert. Auch die Deutsche Bundesbank hat mit dem Projekt „Journey to Cloud" den Aufbau einer hybriden Cloud-Architektur begonnen – ein Signal, das bei den Instituten ankommt.

Leasing-Institute sehen sich auf dem Weg zur Öffnung und Flexibilisierung ihrer IT-Infrastruktur mit Cloud-Strategien allerdings weiterhin mit regulatorischen Hürden konfrontiert. Durch die Veröffentlichung der 6. MaRisk-Novelle sowie den Konkretisierungen in den Bankaufsichtlichen Anforderungen an IT (BAIT) vom 16. August 2021 fordert der Regulator nochmals höhere Aufmerksamkeit der Leasing-Gesellschaften für die operative Informationssicherheit und das regulatorische Auslagerungsmanagement. Cloud-Strategien sind von diesen erhöhten Anforderungen unmittelbar betroffen, da sie fast immer mit einer geteilten Nutzung von Ressourcen und damit zusätzlichen Risiken der Informationssicherheit sowie der Auslagerung von Diensten an IT-Provider verbunden sind.

Cloud-Dienste nicht verteufeln

Regulatorische Anforderungen müssen einer Cloud-Strategie allerdings nicht im Wege stehen. Ganz im Gegenteil: Die Nutzung von Software und IT-Infrastruktur als „Managed Service" kann dabei helfen, die Komplexität in der IT-Organisation zu reduzieren, die Leistungsfähigkeit zu steigern und höchste Branchenstandards zur Informationssicherheit zu erfüllen.

Da sich die öffentliche Wahrnehmung beim Thema Cloud stark auf die Risiken durch die Verwendung geteilter Ressourcen, wie beispielsweise Rechenleistung und Speicherplatz, fokussiert, wird gerade die Informationssicherheit häufig als Nachteil von Cloud-Lösungen angeführt. Das wird modernen Cloud-Technologien nicht gerecht. Während Risiken aus Cyberangriffen und sonstigen Sicherheitsvorfällen in den vergangenen Jahren zunehmend gestiegen sind, haben die großen Cloud-Provider massiv in den Schutz ihrer Infrastruktur investiert. Mehrere tausend Expertinnen und Experten für Cybersicherheit und intelligente Sicherheitsfunktionen, die mitunter auf künstlicher Intelligenz beruhen, ermöglichen ein hohes Niveau an Cybersicherheit für die Unternehmensressourcen in der Cloud. Bei einer detaillierten Analyse werden die Institute feststellen, dass die Sicherheitsstandards ihrer eigenen On-Premises-Lösungen häufig nicht das Niveau der etablierten Cloud-Provider erreichen.

CLEMENS NAWROTH

ist Senior Manager bei zeb Consulting, Hamburg.

E-Mail:
clemens.nawroth@zeb.de

DR. KLAUS STRENGE

ist Partner bei zeb Consulting, Münster.

E-Mail:
klaus.strenge@zeb.de

Ergänzend hierzu bieten die großen Cloud-Provider standardisierte Prozesse und branchenübliche Zertifizierungen für das Informationssicherheitsmanagement an. Ein hoher Grad an Professionalisierung und Standardisierung reduziert die Hürden in der Zusammenarbeit.

Trotzdem gilt es, Risiken aus Cloud-Technologien nicht zu unterschätzen und im Informationsrisikomanagement angemessen zu berücksichtigen. Beispielweise können Sicherheitslücken in der Cloud-Plattform dazu führen, dass Institute Opfer von Cyberangriffen werden, die zunächst gar nicht im Fokus der Angreifer standen. Bekannte Sicherheitslücken in geteilten Ressourcen sind eine Gefahr für alle Instanzen auf der Cloud-Plattform.

Zudem erfordert die Nutzung von öffentlichen Cloud-Services eine stärkere Öffnung des Firmennetzwerks, da die Cloud-Dienste im Gegensatz zu einem geschlossenen Netzwerk bei On-Premises-Lösungen über das Internet bezogen werden. Das gilt insbesondere dann, wenn Cloud-Services als Ergänzung zu on-premises-betriebenen Anwendungen eingesetzt werden. Öffnungen von Ports des Rechenzentrums für eine Kommunikation zwischen Cloud-Services und On-Premises-Anwendungen können neue Angriffspunkte und damit Informationssicherheitsrisiken darstellen.

Folglich ist eine institutsspezifische Abwägung von Chancen und Risiken bei der Nutzung von Cloud-Technologien notwendig. Neben den thematisierten Aspekten der operativen Informationssicherheit sind weitere Facetten der neuen Technologien in Bezug auf deren Chancen und Risiken zu berücksichtigen. Dazu zählen beispielsweise die Themen Datenschutz, Notfallmanagement, Auslagerungsmanagement, Mitarbeiterqualifizierung und Potenziale in der Geschäftsentwicklung durch eine Flexibilisierung von IT-Services.

Allein schon aufgrund dieser Abwägung kann der Weg in die Cloud niemals eine rein operative Entscheidung der IT-Organisation sein. Die Nutzung von Cloud-Technologien betrifft alle Bereiche eines Leasing-Instituts. Dies verdeutlichen folgende Beispiele:

- In der IT-Organisation sind neue Fähigkeiten und Kenntnisse erforderlich, um den Technologie-Stack kontinuierlich zu adjustieren und den Provider zu steuern.
- Die Geschäftsbereiche können eine höhere Leistungsfähigkeit der IT und eine schnellere Time-to-Market innovativer Lösungen erwarten und sollten ihre fachlichen Anforderungen an die IT darauf ausrichten.
- Das Informationssicherheits- und Risikomanagement muss die veränderte Bedrohungslage evaluieren und die IT-Risiken quantifizieren.

Strategische Entscheidung

Die Entscheidung zugunsten von Cloud-Technologien sollte daher immer einem strukturierten Strategieprozess folgen. Gegebenenfalls ist die Geschäftsstrategie, mindestens aber die IT-Strategie des Leasing-Instituts zu überarbeiten. In der IT-Strategie ist eine detaillierte Beschreibung der strategischen Ziele erforderlich. So kann es beispielsweise für ein Leasing-Unternehmen sinnvoll sein, zunächst nur einen Teil der IT-Services in einer Cloud zu betreiben und weitere Applikationen im herkömmlichen On-Premises-Rechenzentrum zu hosten.

Auch ist zu entscheiden, ob das Institut eine eigene Cloud-Umgebung (Private Cloud) betreiben möchte, oder die öffentlichen Cloud-Dienste (Public Cloud) eines IT-Dienstleisters nutzt. Hybride Ansätze durch eine Kombination von einer oder mehreren Public Clouds mit einer oder mehreren Private Clouds sind ebenfalls denkbar. Allen Bereitstellungsmodellen ist gemeinsam, dass Ressourcen gepoolt werden und dadurch eine flexible Bereitstellung und Skalierung von Services möglich wird.

Aus regulatorischer Sicht sind jegliche Ansätze vertretbar, solange eine dezidierte Analyse der Vor- und Nachteile zu einer für Dritte nachvollziehbaren Entscheidung der Geschäftsleitung führt.

Die IT-Strategie sollte nicht nur die strategischen Ziele im Hinblick auf die Cloud enthalten, sondern auch die spezifische Ausrichtung der IT-Organisation auf diese neuen Ziele. Ausgangspunkt ist der Grad der Nutzung verschiedener Cloud-Dienste, wie beispielsweise Software-as-a-Service, In-

frastructure-as-a-Service und Platform-as-a-Service. Daraus ergeben sich mittel- und langfristige Änderungsbedarfe für das Informationssicherheitsmanagement, das IT-Notfallmanagement, die personellen, finanziellen und sonstigen Ressourcen in der IT-Organisation sowie die Budget- und Kostenplanung.

Die spezifische Ausrichtung der IT-Organisation wird zudem von einer neuen Bedrohungslage geprägt. Die Schattenseiten von vernetzten und offenen Plattformtechnologien sind die bereits angesprochenen Cyber-Risiken. Leasing-Unternehmen müssen sich daher verstärkt mit operativen Maßnahmen zur kontinuierlichen Überwachung und zur Härtung der Cloud-Architektur auseinandersetzen – Ziele, die in einer IT-Strategie zu konkretisieren sind.

Die IT-Risikosituation wird allerdings keineswegs ausschließlich negativ geprägt. Chancen ergeben sich beispielsweise durch die gezielte Nutzung von „Containerization" im Kontext des IT-Notfallmanagements. Durch eine Entkopplung von Systemen lassen sich Ausfälle gänzlich vermeiden oder Wiederanlaufszenarien flexibler umsetzen. Ein dezentrales Design von Systemen sowie eine gesteuerte Ressourcenverteilung durch externe „Load Balancer" ermöglichen das gezielte An- und Abschalten schadhafter Komponenten in mehreren virtuellen (und sogar physischen) separierten Umgebungen, ohne dass die darauf basierenden Geschäftsprozesse in ihrer Verfügbarkeit gestört werden.

In der Praxis bleibt die IT-Strategie von Instituten häufig zu unpräzise. Es fehlt eine klare Roadmap für die Umsetzung der Ziele. Daneben fehlen konkrete Key-Performance-Indicators (KPIs) für die Messung der Zielerreichung. Ohne Roadmap und ohne KPIs ist keine Steuerung der Strategieumsetzung möglich. Institute sollten daher das notwendige Level der Konkretisierung ihrer IT-Strategie erreichen und in ein Regelreporting an die Geschäftsleitung überführen.

Einhaltung regulatorischer Anforderungen

Ist die Cloud-Strategie definiert, beginnen die eigentlichen regulatorischen Herausforderungen. Finanzinstitute müssen selbstverständlich auch bei Cloud-Auslagerungen sämtliche gesetzlichen und regulatorischen Regelungen erfüllen. Dazu gehören insbesondere die Mindestanforderungen an das Risikomanagement (MaRisk), die Bankaufsichtlichen Anforderungen an die IT (BAIT) in Kombination mit weiteren Anforderungen aus der Datenschutz-Grundverordnung sowie den Empfehlungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) aus der „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter".[1)]

Mittels einer Governance für Cloud-Auslagerungen können Institute organisatorisch sicherstellen, dass neben den regulatorischen Anforderungen auch die institutsindividuellen Anforderungen an Cloud-Dienste erfüllt werden. Die Cloud Governance erstreckt sich auf die Anbahnung neuer, das Management laufender sowie die Beendigung bestehender Cloud-Dienste. Dabei regelt sie den organisatorischen Aufbau, Prozesse sowie Methoden und Verfahren, die spezifisch für Cloud-Auslagerungen Anwendung finden.

Bereits bei der Providerauswahl und Vertragsverhandlung werden die Weichen für eine gesetzliche und regulatorische Compliance gestellt. Deshalb ist die Definition eines Verfahrens für die Anbahnung neuer Cloud-Auslagerungen ein wichtiger Bestand der neuen Governance. Institute erhalten mit dem „Kriterienkatalog Cloud Computing C5"[2)] des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie der bereits angeführten „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter" der BaFin einen nützlichen Rahmen für das Verfahren. Diesen gilt es dann, institutsindividuell auszugestalten.

»Institute sollten Kriterien definieren, wann eine Dienstleistung als Cloud-Dienst einzustufen ist.«

In der Praxis stellt sich schon zu Beginn die Frage, wann eine Cloud-Auslagerung vorliegt. Die Orientierungshilfe der BaFin definiert Cloud-Dienste als „Dienste, die mithilfe von Cloud-Computing erbracht werden, das heißt ein Modell, das ortsunabhängigen, komfortablen und bedarfsgesteuerten Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Rechenressourcen ermöglicht (wie Netzwerke, Server, Speicher, Anwendungen und Services) und sich schnell sowie mit einem Mindestmaß an Verwaltungsaufwand oder Interaktion des Dienstleisters implementieren und freischalten lässt."

Dabei unterscheidet die BaFin zwischen drei Dienstleistungsmodellen für Cloud-Dienste

- Infrastructure-as-a-Service (IaaS, Bereitstellung von Rechenleistungen und Speicherplatz)
- Platform-as-a-Service (PaaS, Bereitstellung von Entwicklerplattformen)
- Software-as-a-Service (SaaS, Bereitstellung von Softwareapplikationen/Webanwendungen)

sowie vier Bereitstellungsmodellen

- **Private Cloud:** Cloud-Infrastruktur, die ausschließlich von einem einzelnen Unternehmen genutzt werden kann
- **Community Cloud:** Cloud-Infrastruktur, die ausschließlich von einer abgegrenzten Unternehmensgemeinschaft genutzt werden kann, einschließlich mehrerer Unternehmen innerhalb einer Gruppe,
- **Public Cloud:** Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann

› **Hybrid Cloud:** Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt[3)]

Die Anforderungen der BaFin an Cloud-Dienste im Kontext des Auslagerungsmanagements gelten grundsätzlich für alle Dienstleistungs- und Bereitstellungsmodelle. Explizit hervorgehoben seien an dieser Stelle die Private Cloud und die Community Cloud, welche intuitiv nicht als klassischer Cloud-Dienst charakterisiert werden. Dennoch fallen auch diese Bereitstellungsmodelle unter die Begriffsdefinition der BaFin.

Gerade bei diesen Bereitstellungsmodellen ist die Abgrenzung zum herkömmlichen On-Premises-Hosting mitunter schwierig. Institute sollten daher konkrete Kriterien definieren, wann eine Dienstleistung als Cloud-Dienst einzustufen ist. Bei dieser Prüfung sind auch Weiterverlagerungen aufseiten des IT-Dienstleisters zu berücksichtigen, sollte dieser auf einen Cloud-Anbieter zurückgreifen, um eine wesentliche Funktion wahrzunehmen.

Das BSI bedient sich zur Charakterisierung von Cloud-Diensten[4)] der Definition des US-amerikanischen National Institute of Standards and Technology, das ein zu ISO 27001 vergleichbares Framework zur Informationssicherheit anbietet. Danach sind Cloud-Dienste vor allem dadurch gekennzeichnet, dass die bereitgestellten Ressourcen in einem Pool liegen, „on-demand" zur Verfügung gestellt werden und hochskalierbar sind.

In der Cloud ist vor der Cloud

Der Weg in die Cloud ist erst der Anfang einer strategischen Reise in der Welt moderner Technologien. Nach der Migration von Anwendungen in die Cloud-Infrastruktur müssen die Chancen der Cloud für die Weiterentwicklung des Geschäftsmodells nutzbar gemacht werden bei gleichzeitiger laufender Einhaltung regulatorischer und gesetzlicher Anforderungen.

Die Zeit nach der Cloud-Migration sollte daher bereits mit der Entscheidung für eine Cloud-Auslagerung im Sinne einer strategischen und regulatorischen Roadmap geplant werden. Dabei können die nachfolgenden Leitfragen als unterstützende Anhaltspunkte herangezogen werden:

› Welche Person oder welcher Funktionsbereich in der Organisation wird für das Management der Cloud-Auslagerungen verantwortlich sein – sowohl fachlich als auch regulatorisch?

› Wie ist prozessual sichergestellt, dass sich ändernde gesetzliche und regulatorische Anforderungen bei bestehenden Cloud-Auslagerungen Berücksichtigung finden?

› Welche Weiterbildungsmaßnahmen für Mitarbeiterinnen und Mitarbeiter in der IT sowie weiteren Fachbereichen sind notwendig?

› Welche neuen Risiken entstehen durch eine Cloud-Auslagerung für das Institut und mit welchen Maßnahmen können diese schrittweise minimiert werden?

› Wie wird aus den vorhanden Cloud-Technologien ein echter Kundennutzen?

› Welche weiteren IT-Services können und sollten schrittweise in die Cloud verlagert werden?

Damit ist auch klar, dass nicht gleich mit Beginn der Cloud-Auslagerung alle Herausforderungen für die Organisation final gelöst sein müssen. Sie sollten jedoch transparent und in der Planung berücksichtigt sein. Das ermöglicht einen initialen Schritt in die Cloud in einem vernünftigen Zeit- und Budgetrahmen.

Fußnoten
1) BaFin, Orientierungshilfe der BaFin zu Auslagerungen an Cloud-Anbieter, 2018.
2) BSI, Kriterienkatalog Cloud Computing C5, 2020.
3) BaFin, 2018.
4) BSI, 2020.