



zeb

ZEB-PERSPEKTIVE

Cloud or out – Cloud-Technologie jetzt nutzen

partners for change

Zentrale Erkenntnisse

- 1** Der Einsatz von **Cloud-Technologien** ist **unausweichlich**. Dabei ist die IT- und Prozessmodernisierung für Banken und Finanzdienstleister die zentrale Herausforderung.
- 2** Nur wenn Prozess- und IT-Architektur mit aktuellen Digitaltechnologien zukunftsfähig ausgerichtet werden, kann eine **Bank mit dem Markt Schritt halten**.
- 3** Durch den iterativen Einsatz von Cloud-Lösungen eignen sich Organisationen das Wissen an und entwickeln Kompetenzen, aus denen **Wettbewerbsvorteile** entstehen.
- 4** Für den Cloud-Einsatz gibt es **keine K.-o.-Kriterien** – die Rahmenbedingungen sind wichtig, aber bei systematischer Berücksichtigung beileibe keine Show-Stopper.
- 5** „Kosten senken“ ist das Hauptargument für die Cloud. Dabei kann sie weitaus mehr für die **Zukunftssicherheit** eines Instituts leisten.

Gut zu wissen

Cloud or out? Vor zwei Jahren wäre man für diese steile These noch belächelt worden, zumindest in deutschen IT-Abteilungen. Inzwischen hat sich aber auch hierzulande der Markt entwickelt: Immer mehr Unternehmen gehen den Schritt vom begrenzten Cloud-Piloten zu einer umfassenderen Nutzung dieses Bereitstellungsmodells.

Allmählich erodieren die starren Grenzen der eigenen Rechenzentren und ihrer traditionellen Betriebsstrukturen. Das Schlagwort „Cloud“ jedenfalls hat seinen Schrecken weitgehend verloren: Risiken wie potenzieller Kontrollverlust, Geheimnisverrat und Lock-in lassen sich durch passende Strategien beherrschen und wiegen daher heute weniger schwer als die vielen Vorteile, die ein Umstieg mit sich bringen kann.

Schließlich umfasst das Gesamtpaket Cloud weitaus mehr als die reine Kostendimension: Schrittweises Lernen, größere Flexibilität, eine kürzere Time-to-Market und zeitgemäße Security-Maßnahmen sind Ziele, die jede kundenorientierte IT erfüllen muss. Und Fachbereiche sehen immer häufiger, dass Cloud woanders funktioniert, ohne dass Unternehmen gleich wie ein Kartenhaus zusammenfallen. Das weckt Begehrlichkeiten, die nicht ignoriert werden können.

Vor zwei Jahren half hier noch die rechtliche Drohkulisse, um bei der Cloud auf Zeit zu spielen. Bei näherer Betrachtung zeigt sich jedoch, dass die Rahmenbedingungen inzwischen kein Show-Stopper sind, sondern ein Regulativ, das beherrschbar ist. Mehr Argumente dazu finden Sie im weiteren Verlauf dieser Publikation.

Public Cloud – Umsatzprognose weltweit

Mrd. USD

400

300

200

100

0

2019

2020

2021

2022

Business Process as a
Service (BPaaS)

Software as a Service
(SaaS)

Platform as a Service
(PaaS)

Infrastructure as a Service
(IaaS)

Cloud-Technologien sind unausweichlich

Modernisierung der IT und Prozesse als zentrale Herausforderung für die Nutzung der Chancen

Die IT entscheidet als kritischer Produktionsfaktor und moderne Kundenschnittstelle maßgeblich über den Erfolg ganzer Geschäftsmodelle. Daher rückt sie – berechtigterweise – zunehmend in den Gestaltungsmittelpunkt. Die Entwicklung gipfelt in der These, dass Banken sich primär zu Technologieunternehmen entwickeln müssen. Unabhängig davon, wie man zu dieser radikalen

Forderung steht, ist eine zukunftsfähige Ausrichtung der Prozess- und IT-Architektur unter Einsatz aktueller Digitaltechnologien unausweichlich, um im Markt Schritt halten zu können. Dazu zählt auch, dass Finanzdienstleister jetzt mit der Nutzung von Cloud-Technologie beginnen müssen.

„Eine zukunftsfähige Ausrichtung der **Prozess- und IT-Architektur** unter Einsatz aktueller **Digital-technologien** ist unausweichlich.“

Dr. Wolf Behrmann,
Senior Manager, zeb



Cloud eröffnet sechs Potenzialbereiche

Höhere Flexibilität und kürzere Time-to-Market

Cloud-Services betreiben IT-Leistungen und stellen sie hoch automatisiert über vollständig virtualisierte Rechenzentrumskomponenten bereit. Zusätzliche Komponenten wie ein weiterer Prozessor oder sogar ganze Computernetzwerke können binnen Minuten ergänzt werden. Dadurch bieten Cloud-Services eine hohe Flexibilität in der Umsetzung von fachlichen Anforderungen, erhöhen die Geschwindigkeit und reduzieren die Risiken. Neue Anforderungen und Produkte lassen sich so schnell – ohne die traditionellen Rüstzeiten – an den Markt bringen.

Mehr Kundennähe und schnelles Feedback

Entwicklerinnen und Entwickler können berechtigt werden, Projektinfrastruktur eigenständig in der Cloud zu buchen. Vorlauf- und Wartezeit werden so deutlich reduziert, und Kosten können dem verursachenden Projekt zugewiesen werden. Unsere Erfahrungen zeigen, dass sich allein dadurch die Durchlaufzeiten im Entwicklungsprozess um 10 bis 15 Prozent reduzieren lassen. Durch die Nutzung moderner cloudbasierter Entwicklungsprozesse kann zusätzlich die Kundennähe deutlich verbessert werden. Anforderungen lassen sich schnell umsetzen und an den Kunden ausrollen, um direkt Feedback aus dem Markt zu bekommen. So wird eine gute und laufend weiterentwickelte User-Experience erreicht, die zum entscheidenden Wettbewerbsvorteil werden kann und sich zunehmend zum essenziellen „Hygienefaktor“ entwickelt.

09/1999

Salesforce als erster SaaS-Anbieter gegründet

09/2008

Cloud-Speicherdienst Dropbox geht an den Markt

04/2011

IBM SmartCloud Enterprise Plattform gelauncht

09/2012

Oracle ERP Cloud angekündigt

07/2016

N26 geht mit cloud-basierten Bank-services an den Markt

Innovations- und „Vendor-Phase“

„Early Adopter“-Phase

01/1999

Cloud-Begriff taucht auf

11/2004

AWS steht für öffentliche Nutzung zur Verfügung

02/2010

Microsoft-Azure-Plattform offiziell verfügbar

11/2011

Google Cloud Platform wird generell verfügbar

11/2014

Talanx AG nutzt AWS und gewinnt „Best-in-Cloud-Award“

11/2016

Generali und Microsoft erklären Partnerschaft zu Cloud

drei

Professionalisierung der IT-Security

Das Umfeld IT-Security und IT-Compliance ist ebenfalls zu nennen. Auch hier leisten – anders als initial erwartet – Cloud-Lösungen einen wichtigen Beitrag. Für „Einzelkämpfer“ wird es zunehmend schwieriger, die immer weiter wachsenden Anforderungen und Bedrohungen zu managen. So haben etwa bei DDoS-Attacken große Infrastrukturen mit dezidierten Cyber-Security-Teams deutlich bessere Möglichkeiten, diese zu entschärfen bzw. abzuwehren. Zudem werden durch den hohen Automatisierungsgrad menschliche Fehler bei der Einrichtung der Systemumgebung vermieden. Dies wirkt sich in Summe auf die Produktionssicherheit eines Instituts aus.

vier

Fokus auf das Kerngeschäft

Die Auslagerung von Risiken und sekundären Geschäftsprozessen an externe Dienstleister ermöglicht es Banken, sich konsequent auf das Kerngeschäft zu fokussieren und ihre Profitabilität sowie die langfristige Wettbewerbsfähigkeit zu verbessern. Dabei gewährleistet eine Multicloud-Strategie mit verschiedenen Lieferanten, dass es nicht zu einem Vendor-Lock-in kommt.

03/2017

SocGen wagt sich mithilfe von Amazon und Microsoft in die Cloud

01/2019

BNP Paribas bucht IBM Services für Cloud-Strategie

05/2019

Deutsche Börse arbeitet mit Microsoft-Cloud

09/2019

Deutsche Börse engagiert mit Google Cloud zweiten Cloud-Anbieter

11/2019

Allianz und Microsoft gehen Partnerschaft ein

07/2020

AWS und HSBC vereinbaren Übereinkunft zu Cloud

08/2018

ING verbindet sich mit Google für Cloud

04/2019

Santander setzt auf Microsoft-Cloud

05/2019

ABN AMRO kooperiert mit Microsoft-Cloud

10/2019

Commerzbank startet Cloud-Initiative

07/2020

Deutsche Bank kooperiert mit Google

07/2020

Finanz Informatik und FI-TS arbeiten mit Google Cloud

„Early Majority“-Phase

Ersatz für aussterbende On-Premises-Lösungen

Perspektivisch werden große und marktübliche Applikationen nicht mehr als On-Premises-Version angeboten. Dieser Trend begann mit Salesforce (gegründet: 1999) und betrifft nun auch traditionelle Softwarehersteller wie Microsoft und SAP. Die frühzeitige Nutzung von Cloud-Services dient folglich auch der Sicherstellung langfristiger Kompatibilität.

Realisierung von Kostenvorteilen

Der richtige Einsatz von Cloud-Technologie ermöglicht Kostenvorteile, die gerade in der aktuellen Ertragssituation immer wichtiger werden. Hohe Investitionskosten für die eigene Serverlandschaft werden obsolet, und zuvor gebundenes Kapital wird somit freigesetzt. Durch verbrauchsabhängige Fakturierung können hohe Fixkosten reduziert und ungenutzte Kapazitäten minimiert werden. Die Einsparpotenziale hängen dabei von der Größe und Auslastung der jeweiligen Infrastruktur sowie der Verteilung der Last ab.

Servicemodell

Beschreibung

BPaaS – Business Process as a Service

Bereitstellung von standardisierten und/oder automatisierten Geschäftsprozessbausteinen, die vom Serviceanbieter kontinuierlich optimiert werden

SaaS – Software as a Service

Bereitstellung von Softwareanwendungen über elektronische Netzwerke (einschließlich Anwendungsmanagement und Wartung)

PaaS – Platform as a Service

Bereitstellung erweiterter, plattformspezifischer Services, z. B. für Softwareentwicklungsprozesse, Data Analytics oder Machine Learning

IaaS – Infrastructure as a Service

Bereitstellung von Infrastruktur (z. B. Verarbeitungskapazitäten, Kommunikationsnetze, Speicher) – entweder als dedizierte Hardware oder in Form von „virtualisierten“ Ressourcen

Frühzeitiges Lernen ist ein wichtiger Erfolgsfaktor

Durch den schrittweisen Einsatz von Cloud-Lösungen kann die Organisation das notwendige Wissen sukzessive aufbauen und Kompetenzen entwickeln, die im Laufe der Entwicklung zu Wettbewerbsvorteilen heranwachsen. Auch mit Blick auf die Migrationsrisiken ist es wichtig, ausreichend Raum für das „Ausprobieren und Lernen“ zu lassen. Die klare Empfehlung lautet daher, schnellstmöglich mit der Nutzung von Cloud-Bausteinen zu beginnen.



„Institute sollten 2021 mit Piloten starten, denn schnelle erste eigene Erfahrungen sind wichtig für den Erfolg der Cloud-Reise.“

Matthias Lehneis,
Senior Manager, zeb



Grundsätzliche Bedenken unbegründet

Rahmenbedingungen sind beherrschbar

Obwohl viele Gründe für den Einsatz von Cloud-Technologien sprechen, zögern hiesige Banken nach wie vor, wenn es um die Cloud-Nutzung jenseits von Pilotprojekten geht. Daher ist es an der Zeit, die drei größten Bedenken auszuräumen.

1. Datenschutzbedenken: „Eine Datenschutzkonforme Umsetzung der Cloud ist mit den großen Anbietern unter der EU-DSGVO nicht möglich.“

- Meinung der Kritik: Die in der EU-DSGVO geforderten Rahmenbedingungen lassen sich in Cloud-Umgebungen insbesondere dann nicht konform umsetzen, wenn ich mit großen Anbietern zusammenarbeite, die auch außerhalb der EU agieren.
- Sachlage: Die gesetzlichen, datenschutzrechtlichen Anforderungen sind unabhängig von der Unternehmensgröße des Cloud-Anbieters einzuhalten. Da dieser als Beauftragter stets weisungsgebunden handelt, verbleibt die Hauptverantwortung für die verarbeiteten Daten immer beim auftraggebenden Unternehmen. Dieses ist auch dafür verantwortlich, die weiteren Anforderungen hinsichtlich der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen im Zuge des Cloud-Einsatzes einzuhalten. Hierbei ist zu beachten, dass Daten

seit „Schrems II“ nicht mehr auf der Grundlage des Privacy Shield übermittelt werden dürfen, da das Abkommen vom EuGH am 16. Juli 2020 für unwirksam erklärt wurde.

- Lösungsansatz: Auch unter dem aktuellen „Schrems II“-Urteil des EuGH ist der internationale Datenverkehr weiterhin möglich. Allerdings müssen die Grundrechte der europäischen Bürgerinnen und Bürger beachtet und Schutzmaßnahmen für den Datenaustausch mit den USA ergriffen werden. Wie genau soll das funktionieren? Die von der Kommission im Jahr 2010 beschlossenen Standardvertragsklauseln sind weiterhin wirksam. Allerdings ist zukünftig für jeden Einzelfall zu überprüfen, ob das Schutzniveau für die übermittelten Daten im Drittland im Wesentlichen dem Schutzniveau der EU entspricht, um erforderlichenfalls mehr Garantien zu gewähren. Um die Zulässigkeit der Datenübermittlung aufrechtzuerhalten, sollten deshalb – nach individueller Prüfung der Zulässigkeit des Anwendungsbereichs – die Ausnahmen nach Art. 49 EU-DSGVO Anwendung finden und die verbindlichen internen Datenschutzvorschriften (auch: Binding Corporate Rules, kurz: BCR) für gruppeninterne Datenübermittlungen eingesetzt werden. Insgesamt sollte die aktuelle Rechtslage unter Berücksichtigung des „Schrems II“-Urteils weiter beobachtet werden, da in diesem Zusammenhang weitere Neuerungen zu erwarten sind.

2. Geheimdienstbedenken: „Die US-Regierung sowie US-amerikanische Sicherheits- und Geheimdienste dürfen alle meine Daten lesen und verarbeiten.“

- Meinung der Kritik: Durch US-amerikanische Gesetzgebung können US-Regierung sowie US-amerikanische Sicherheits- und Geheimdienste auf meine Cloud-Daten zugreifen. Dadurch sind meine Daten ungeschützter als in meinem eigenen Rechenzentrum – folglich kann die Sicherheit in der Cloud nicht gewährleistet werden.
- Sachlage: Durch den EU-Standort des Rechenzentrums eines Cloud-Anbieters wird nicht automatisch sichergestellt, dass die geforderten Datenschutzstandards erfüllt werden. Dies liegt daran, dass sich der sog. CLOUD („Clarifying Lawful Overseas Use of Data“) Act nicht auf Unternehmen mit Hauptsitz in den USA beschränkt. Der CLOUD Act regelt ergänzend zum Patriot Act (verpflichtet Unternehmen infolge der Terrorangriffe um den 11. September 2001 u. a. zur Übermittlung von strafrechtlich relevanten Daten an US-Behörden) seit dem Frühjahr 2018 den Zugriff auf in der EU gespeicherte personenbezogene Daten von US-Bürgern und ermöglicht weiter den Zugriff auf Daten von EU-Bürgern in den USA. Er bezieht sich auf Unternehmen weltweit, die eine Niederlassung in den USA

unterhalten oder dort einer Geschäftstätigkeit nachgehen. Damit ist der Blick auf den Unternehmenssitz und den Verarbeitungsstandort nicht mehr ausreichend, um der Sorgfaltspflicht im Rahmen der EU-DSGVO nachzukommen. Da der CLOUD Act die Datenübermittlung nicht davon abhängig macht, ob zwischen dem betroffenen Land und den USA ein Rechtshilfeabkommen besteht, sind EU-Unternehmen durch seine Einführung im Fall der Fälle gezwungen, gegen die EU-DSGVO oder den CLOUD Act zu verstoßen.

- Lösungsansatz: Da Unternehmen, die personenbezogene Daten in der Cloud verarbeiten, sicherstellen müssen, dass sie die in der EU geforderten Datenschutzbestimmungen einhalten, sind die Verträge mit Cloud-Anbietern so anzupassen, dass sie konform mit der EU-DSGVO sind. Aufgrund der geschilderten Sachlage ist es für europäische Unternehmen aktuell am besten, sich für einen europäischen Cloud-Anbieter mit Rechenzentren in der EU zu entscheiden (Best Practice), um das Risiko eines Zugriffs durch die US-Regierung sowie US-amerikanische Sicherheits- und Geheimdienste zu verringern. Es ist zudem vor allem dazu zu raten, dass Daten in verschlüsselter Form gespeichert werden. Der CLOUD Act bietet zwar eine Rechtsgrundlage für Herausgabeverlangen von US-Behörden, nicht aber für eine Entschlüsselung von Daten.

3. Regulierungsbedenken: „Da der Regulator das Thema Cloud kritisch sieht und die Rechtslage unklar ist, können Cloud-Anbieter eine MaRisk-konforme Cloud-Nutzung nicht gewährleisten.“

- Meinung der Kritik: Da in den regulatorischen Anforderungen nicht immer explizit auf den Einsatz von Cloud-Technologien eingegangen wird, sind die Anforderungen nicht präzise und geben Interpretationen Spielraum. Die vom Regulator geforderten Informations- und Prüfungsrechte lassen sich deshalb nicht durchsetzen, Sanktionierungen allein gegen Institute sind unwirksam gegenüber Cloud-Anbietern.
- Sachlage: Der erste Schritt zur Konkretisierung des regulatorischen Rahmens für Cloud-Computing war die Veröffentlichung des Rundschreibens „Bankaufsichtliche Anforderungen an die IT“ (BAIT), welches klarstellte, dass der Auslagerungsabschnitt AT 9 MaRisk auch für die Nutzung solcher Cloud-Dienste gilt, die eine Auslagerung von IT-Dienstleistungen darstellen.

- Lösungsansatz: Beaufsichtigte Unternehmen, welche die Nutzung eines Cloud-Diensts beabsichtigen, müssen vorab prüfen, inwieweit die aufsichtsrechtlichen Anforderungen an Auslagerungen zu beachten sind. Handelt es sich nach Prüfung der Risikogesichtspunkte um eine wesentliche Auslagerung, sind in diesem Zusammenhang bei der Vertragsgestaltung neben §§ 25a und 25b KWG auch AT 9 MaRisk sowie die BAIT einzuhalten. Nur durch den uneingeschränkten Zugang zu den Cloud-Anbietern (beispielsweise zu Geschäftsräumen, Rechenzentren etc.) ist es den beaufsichtigten Unternehmen möglich, ihre Informations- und Prüfungsrechte ordnungsgemäß wahrzunehmen. Die vertragliche Einräumung uneingeschränkter Informations- und Prüfungsrechte vonseiten der Cloud-Anbieter ist daher von enormer Bedeutung. Bei nicht wesentlichen Auslagerungen sind in diesem Zusammenhang die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a KWG zu beachten. Sofern die Nutzung eines Cloud-Diensts als wesentliche Auslagerung eingestuft wird, sind im Auslagerungsvertrag

„Für den sofortigen Cloud-Einsatz gibt es derzeit **keine K.-o.-Kriterien.**“

Caroline Sieveritz,
Senior Consultant, zeb



angemessene Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer als uneingeschränkte Rechte einzuräumen. Solche Vereinbarungen können insbesondere mit den großen Cloud-Anbietern inzwischen problemlos geschlossen werden.

Mit den notwendigen Vorarbeiten lassen sich die typischen Argumente der Kritik und die Bedenken bezüglich der Cloud entkräften. Somit steht auch bei Banken und Finanzdienstleistern der Entwicklung einer individuellen Cloud-Strategie nichts mehr im Wege.

→ Welche Elemente in einer Cloud-Strategie abgedeckt und im Rahmen einer Governance konkretisiert werden müssen, um erfolgreich in die Cloud zu starten, werden wir in einem ergänzenden Artikel publizieren. Dort werden wir auch auf die unterschiedlichen Migrationsstrategien von der heutigen Architektur in ein Cloud-Szenario beleuchten.

Wir sind Partner der Veränderer

zeb ist eine der führenden, auf den Finanzdienstleistungssektor spezialisierten Strategie- und Managementberatungen in Europa

Weitere Publikationen

Wenn Sie mehr erfahren möchten, schreiben Sie bitte eine E-Mail an publications@zeb.de



COVID-19 beschleunigt die digitale Transformation
bit.ly/3ifygng



Data Analytics bei Finanzdienstleistern
bit.ly/3n4r1SP



Data Analytics – verloren geglaubte Kunden aktivieren
bit.ly/3dx4qZ8

Besuchen Sie uns online



zeb-consulting.com



twitter.com | [zeb_consulting](https://twitter.com/zeb_consulting)



linkedin.com | [zeb_consulting](https://linkedin.com/company/zeb_consulting)



xing.com | [zeb](https://xing.com/profile/show/zeb)



youtube.com | [zebconsulting](https://youtube.com/zebconsulting)



instagram.com | [zeb_consulting_](https://instagram.com/zeb_consulting_)



Sven Krämer

Partner

Phone +49.251.97128.385

Mobile +49.151.12054003

sven.kraemer@

zeb-consulting.com

Office Münster



Dr. Wolf Behrmann

Senior Manager

Phone +49.251.97128.664

Mobile +49.15112054036

wbehrmann@zeb.de

Office Münster



Matthias Lehneis

Senior Manager

Phone +49.40.303740.139

Mobile +49.15167879940

mlehneis@zeb.de

Office Hamburg



Caroline Sieveritz

Senior Consultant

Phone +49.89.543433.360

Mobile +49.1754008903

caroline.sieveritz@zeb.de

Office München

Diese Publikation wurde ausschließlich zur allgemeinen Orientierung erstellt und berücksichtigt nicht die individuellen Anlageziele oder die Risikobereitschaft der Leserin/des Lesers. Die Leserin/der Leser sollte keine Maßnahmen auf Grundlage der in dieser Publikation enthaltenen Informationen ergreifen, ohne zuvor spezifischen professionellen Rat einzuholen. zeb.rsa gmbh übernimmt keine Haftung für Schäden, die sich aus einer Verwendung der in dieser Publikation enthaltenen Informationen ergeben. Ohne vorherige schriftliche Genehmigung von zeb darf dieses Dokument nicht in irgendeiner Form oder mit irgendwelchen Mitteln reproduziert oder vervielfältigt werden.

Münster
Hammer Straße 165
48153 Münster, DE
zeb-consulting.com

Amsterdam
Barbara Strozilaan 101,
1083 HN Amsterdam, NL
zeb-consulting.nl

Berlin
Friedrichstr. 78,
10117 Berlin, DE
zeb-consulting.com

Frankfurt a. M.
Taunusanlage 19,
60325 Frankfurt a. M., DE
zeb-consulting.com

Hamburg
Kurze Mühren 20,
20095 Hamburg, DE
zeb-consulting.com

Kiew
42–44 Shovkovychna Str.,
1601 Kiev, UA
zeb-consulting.com

Kopenhagen
Arne Jacobsens Allé 7,
2300 Copenhagen, DK
zeb.se

London
107 Cheapside,
EC2V 6DN London, GB
zeb.co.uk

Luxemburg
37A, Avenue John F. Kennedy,
1855 Luxembourg, LU
zeb.lu

Mailand
Via Santa Maria Segreta 6,
20123 Milan, IT
zeb-consulting.it

Moskau
Testovskaya St., 10,
123112 Moscow, RU
zeb.com.ru

München
Theresienhöhe 13a,
80339 München, DE
zeb-consulting.com

Oslo
Filipstad Brygge 1,
0252 Oslo, NO
zeb.se

Stockholm
Biblioteksgatan 11,
111 46 Stockholm, SE
zeb.se

Warschau
ul. Krolewska 18,
00-103 Warsaw, PL
zeb.pl

Wien
Praterstraße 31,
1020 Vienna, AT
zeb.at

Zürich
Gutenbergstr. 1,
8002 Zürich, CH
zeb.ch