bankenverband

Themenbeitrag
Fragen und Antworten zum Thema Cloud

23. September 2021

Bettina Schönfeld
Associate Director
+49 30 1663 2316
bettina.schoenfeld@bdb.de

Das Thema Cloud-Technologie bzw. Auslagerungen in die Cloud gewinnt immer mehr an Bedeutung – auch im Bankenumfeld. Auf dieser Seite beantworten wir die wichtigsten Fragen zur Auslagerung in die Cloud, zur Datensicherheit und zur Datenspeicherung.

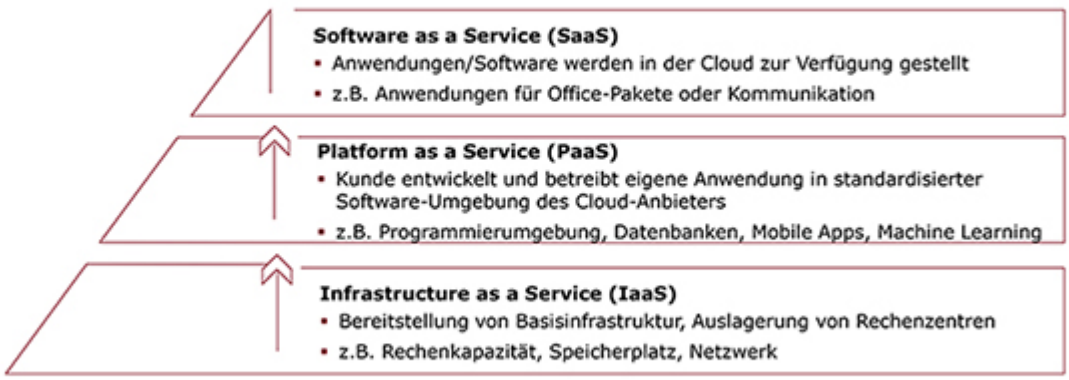
Auslagerung in die Cloud

Wann spricht man von einer Auslagerung?

Von einer Auslagerung wird immer dann gesprochen, wenn ein externes Unternehmen mit der Wahrnehmung von Aktivitäten und Prozessen beauftragt wird, die Bestandteil von Bankgeschäften, Finanzdienstleistungen (siehe § 1 KWG) oder sonstigen institutstypischen Dienstleistungen sind und ansonsten vom Institut selbst erbracht würden.

Welche Möglichkeiten gibt es, Auslagerungen an Cloud-Dienstleister vorzunehmen?

Es wird grundsätzlich zwischen drei Diensten bei der Auslagerung an Cloud-Dienstleister unterschieden (siehe Abbildung).



Bei Infrastructure-as-a-Service (IaaS) handelt es sich um die Basis der drei Cloud-Dienste. Hierbei werden Hardwarekomponenten für den Benutzer bereitgestellt, auf die er online zugreifen kann. Dies kann sowohl Speicherplatz für eine große Menge abzulegender Dateien sein als auch flexible Rechenka-

pazität für umfangreiche Rechenleistungen bei schwankenden Zugriffszahlen auf einen Webshop.

Platform-as-a-Service (Paas) bietet dagegen neben der Hardware auch eine umfangreiche, standardisierte Software-Umgebung, welche zur einfachen Erstellung von mobilen Apps oder zum Einsatz von Tools für künstliche Intelligenz und die Analyse großer Datenmengen genutzt werden kann.

Bei Software-as-a-Service (SaaS) wird eine einsatzbereite Softwareanwendung für Endnutzer bereitgestellt. Die Software wird gegen eine Gebühr genutzt, wechselt dabei aber nicht den Eigentümer. Die Anwendung wird über die Cloud bereitgestellt und kann jederzeit und mit verschiedensten Endgeräten genutzt werden. Der Nutzer stellt im Prinzip nur noch die Daten für die Anwendung zur Verfügung.

Was ist der Unterschied zwischen Public und Private Cloud?

In der Praxis gibt es verschiedene Bereitstellungsmodelle von Cloud-Diensten, so z.B. die Private und Public Cloud:

- Public Cloud: Services wie Rechenleistung, Infrastruktur, Speicherplatz oder Anwendungen können von einer Vielzahl von Anwendern über das Internet genutzt bzw. gemietet werden.
- Private Cloud: Dienste in der Private Cloud werden nur einem eingeschränkten Benutzerkreis, beispielsweise einzelnen Organisationen zur Verfügung gestellt. Je nach Ausprägung können diese auf eigenen Rechnern oder auf Servern von externen Anbietern betrieben werden. Der Zugriff auf diese Cloud-Dienste erfolgt entweder über das Intranet oder über ein Virtual Private Network (VPN).

Warum lagern Banken Dienstleistungen in die Cloud aus?

Zehn Gründe für die Nutzung von Cloud-Dienstleistungen finden Sie hier.

Was muss eine Bank beachten, wenn sie Dienstleistungen an einen Cloud-Dienstleister auslagert?

Die Auslagerung und Nutzung von Cloud-Dienstleistungen müssen immer in die gesamte IT-Strategie eingebunden sein. Es müssen daher Vorkehrungen getroffen werden, um die umfangreichen gesetzlichen Vorgaben zur Sicherheit, technischen Verfügbarkeit sowie bezüglich weiterer Anforderungen zu gewährleisten. Daneben muss die Bank einen Prozess entwickeln und dokumentieren, der alle für die Auslagerung an den Cloud-Anbieter relevanten Schritte von der Strategie über die Migration in die Cloud bis hin zur Exit-Strategie abdeckt.

Datensicherheit

Wonach richtet sich die Sicherheit der Daten?

Generell setzen Banken und Cloud-Dienstleister hohe Sicherheitsvorkehrungen ein, um Daten zu schützen. Dazu gehören unter anderem verteilte Rechenzentren und technische Absicherungen wie eine entsprechende Verschlüsselung der Daten.

Die Sicherheitsvorkehrungen der Bank und der Cloud-Dienstleister sind abhängig von den Dateninhalten in der Cloud. Dabei wird von einem risikobasierten Ansatz ausgegangen, so dass sich die Maßnahmen nach dem jeweiligen Risikoprofil (Schwere des Risikos und Eintrittswahrscheinlichkeit) richten. Es gilt das Prinzip der Verhältnismäßigkeit, d.h., die Maßnahmen sollten erforderlich, geeignet und angemessen sein. Neben dem Risiko spielen somit auch wirtschaftliche Aspekte wie z.B. Implementierungskosten eine entscheidende Rolle. Eine Auslagerung des Kantinenplans unterliegt z.B. einem anderen Risiko als die Auslagerung von Geschäftsprozessen und wird daher auch in der Risikobetrachtung und Absicherung anders bewertet.

Wie werden die Daten gesichert?

Bei der Datensicherheit gibt es verschiedene Formen der Absicherung. Dazu folgende Beispiele:

- Technische Maßnahmen
  - Pseudonymisierung der Daten und/oder
  - Verschlüsselung der Daten

- Organisatorische Maßnahmen
  - Handlungsanweisungen beispielsweise in Form von Zutritts- und Zugriffskontrollen für Mitarbeiter sowie
  - Protokollierung / Kontrolle der Einhaltung der Anweisungen und
  - vertragliche Maßnahmen durch Vereinbarungen zwischen Cloud-Anbieter und Cloud-Nutzer

Vertrauliche Daten, die über einen Cloud-Dienst ausgetauscht oder in einem Cloud-Backup gesichert sind, liegen in der Regel an jedem Speicherort in verschlüsselter und/oder pseudonymisierter Form vor. Dabei werden die Daten vor dem Übertragen in die Cloud bereits verschlüsselt. Den Schlüssel – und damit den Zugriff auf die Daten – hat nur der Cloud-Nutzer beziehungsweise derjenige, dem die Daten gehören. Der Cloud-Dienstleister kann diese Daten nicht lesen.

Wenn die Daten in der Cloud jedoch auch verarbeitet werden sollen, müssen sie in der Cloud entschlüsselt werden. In diesem Fällen wird durch Verträge zwischen dem Cloud-Nutzer und dem Cloud-Anbieter festgelegt, wer, wann und in welcher Form Zugriff auf die Daten haben darf. So wird sichergestellt, dass

kein Zugriff von unberechtigten Dritten erfolgen kann. Dabei ist in der EU immer die Datenschutz-Grundverordnung (DSGVO) zu beachten.

Für den Transport von Daten in die Cloud ist ein verschlüsselter Cloud-Zugang mittlerweile State of the Art und wird auch im Rahmen von entsprechenden Sicherheitsempfehlungen des Bundesamtes für Informationssicherheit (BSI) oder der Cloud Security Alliance gefordert. Zudem können Unternehmen die Cloud-Zugänge und den Datentransfer in die und aus der Cloud über VPN-Lösungen (Virtual Private Network) absichern.

Wie werden die Daten verschlüsselt?

In der Praxis wird oft auf eine Public-Key-Infrastruktur zurückgegriffen. Der Empfänger veröffentlicht einen öffentlichen Schlüssel, den Public Key. Mit dem Public Key kann nur verschlüsselt, nicht jedoch entschlüsselt werden. Der Sender kann nun die Nachricht mit diesem Public Key verschlüsseln und dem Empfänger zusenden. Der Empfänger besitzt als Einziger den privaten Schlüssel, also den Private Key, und kann daher auch nur die Nachricht entschlüsseln. Grundsätzlich soll eine sichere Ende-zu-Ende-Verschlüsselung die Daten schützen und einen Zugriff durch Dritte verhindern.

Datenspeicherung

Wo liegen die Daten?

Bei großen Cloud-Infrastrukturanbietern werden Daten in mehreren Rechenzentren und Regionen zeitgleich gespeichert. Dies hat den Vorteil, dass Risiken durch Störungen, Cyber-Attacken oder sonstige Probleme minimiert werden. Die Daten gehen nicht verloren und ein Zugriff ist weiterhin jederzeit möglich.

Wo dürfen Daten liegen?

Es wird im Vertrag zwischen der Bank und dem Cloud-Anbieter geregelt, wo die Daten liegen dürfen. Je nachdem, ob die Daten innerhalb der EU oder in einem Drittstaat verarbeitet werden, gibt es unterschiedliche Sicherheits- und Datenschutzanforderungen bei der Datenverarbeitung und -speicherung.

Sind personenbezogene Daten betroffen, ist in der Europäischen Union die Datenschutzgrundverordnung (DSGVO) zu beachten. Dies sind Informationen über natürliche Personen. Daten, die keinen Personenbezug haben oder nur Informationen über juristische Personen enthalten, sind nicht vom Datenschutzrecht erfasst.

Welche Besonderheiten gibt es bei der Nutzung von Cloud-Anbietern in Drittstaaten, wenn personenbezogene Daten betroffen sind?

Während es innerhalb des EU-/EWR-Raums egal ist, in welchem EU-Mitgliedstaat der Anbieter die personenbezogenen Daten verarbeitet, sind bei einer Datenverarbeitung im Drittstaat besondere Vorgaben zu beachten. Grundsätzlich muss der Cloud-Anbieter im Drittstaat ein der DSGVO adäquates Datenschutzniveau gewährleisten. Dazu bietet das EU-Recht Instrumente, wie z.B. die Absicherung per EU-Standardvertragsklauseln. Je nach Datenschutzniveau im jeweiligen Drittstaat können zusätzliche Schutzmaßnahmen erforderlich sein.

Insbesondere der Austausch mit US-basierten Cloud-Dienstleistern ist nach wie vor eine Herausforderung für Unternehmen und Banken. Durch vermeintlich extensive Zugriffsmöglichkeiten der US-Behörden (insbesondere US-Geheimdienste) auf Datenbanken gibt es eine intensive Diskussion über die Gewährleistung des Datenschutzes. Die EU-Kommission hatte bereits Regelungen mit den USA zum Schutz personenbezogener Daten vereinbart, die jedoch 2020 vom Europäischen Gerichtshof für ungültig erklärt wurden. Zuletzt wurden im Juni 2021 neue Standardvertragsklauseln zum Datenschutz von der Europäischen Kommission veröffentlicht. Diese Musterverträge sind ein wichtiger Fortschritt, entbinden Unternehmen und Banken jedoch nicht vor weiteren Prüfungen des tatsächlichen Datenschutzniveaus. Für eine entsprechende Rechtssicherheit sind weitere Instrumente und Leitlinien des EU-Gesetzgebers notwendig.