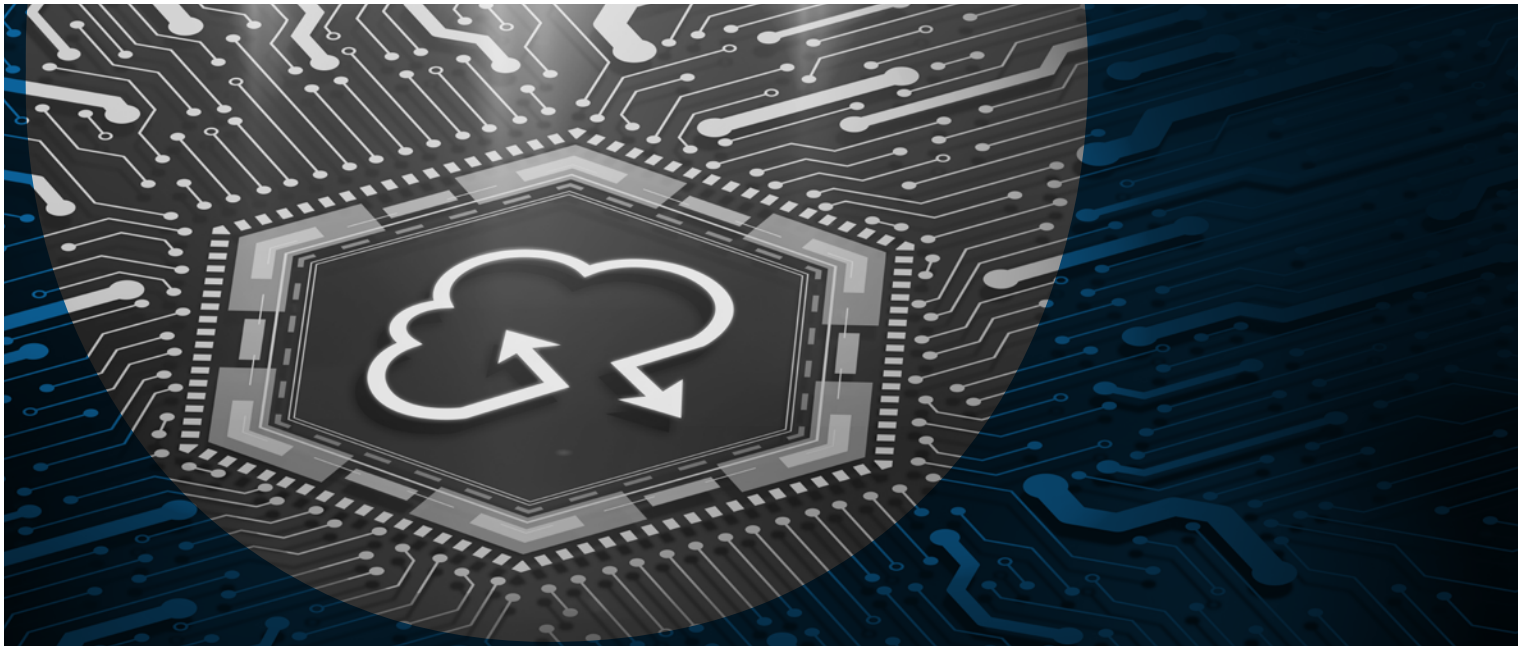


Cloud Banking – Hybrid

Hybrid Cloud – das Beste zweier Welten?

Public oder Private? Beide Cloudmodelle haben Vorteile – aber auch Nachteile, die bestimmte Nutzungsszenarien erschweren. Die Alternative: Hybrid Cloud. Mit dieser Lösung bewahren Banken die Business-Continuity und bekommen gleichzeitig die notwendige Agilität und Sicherheit zur Bewältigung der eigenen digitalen Transformation.

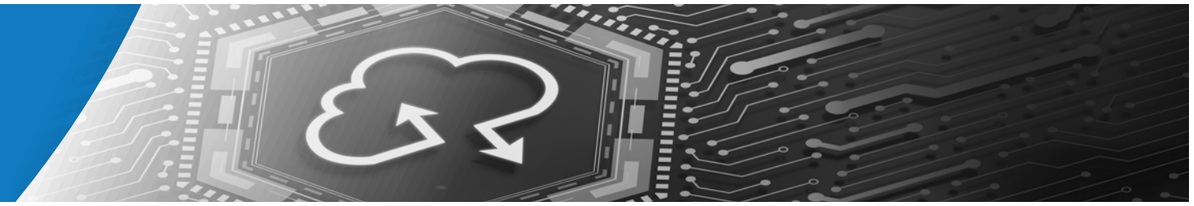
Die Ausgangslage: Welches Cloudmodell passt?

Bei Cloudprojekten ist relativ früh eine wichtige Entscheidung zu treffen: Public oder Private Cloud? Erstere ist in der Regel das Mittel der Wahl, wenn es um Kosteneinsparung, Skalierbarkeit und den Zugang zu neuen und schnelllebigen Technologien geht. Eine Private Cloud bietet dagegen bessere Kontrolle und kann stärker nach den eigenen Anforderungen gestaltet werden. Allerdings sind der Auslagerung sensibler Daten in die Public Cloud regulatorische Grenzen gesetzt.

Inzwischen entscheiden sich daher immer mehr Banken für eine Mischform, die Hybrid Cloud. Dabei werden bei Spitzenlasten gegebenenfalls Prozesse von der Private in die Public Cloud verlagern, oder auch umgekehrt. Dies setzt allerdings eine flexible Auslegung der Prozesse voraus. Ganz unproblematisch sind solche Ansätze nicht. Denn sie bedeuten für Banken einen hohen administrativen Aufwand.

Hybrid Cloud: Herausforderung Datenschutz und Sicherheit

Egal an welchen Dienstleister mit welchem Modell ausgelagert wurde, die Bank bleibt immer und überall für die Einhaltung der regulatorischen Vorgaben verantwortlich. Entsprechend wichtig sind klare Regelungen zu IT-Sicherheit und Datenschutz. Das gilt auch und vor allem, wenn sich die Bank für eine hybride Cloudlandschaft entscheidet. Denn es muss immer nachvollziehbar sein, wer auf die Daten zugreift und wo welche Daten verarbeitet werden. Vor allem Open-Banking-Ansätze bergen immer die Gefahr von Datenlecks. Das liegt an der großen Zahl externer Service-Dienstleister. Es muss sichergestellt sein, dass die EU-Datenschutzverordnung (EU-DSGVO) eingehalten wird. Hinzu kommen Themen wie Software-Deployment oder Portabilität von Infrastruktur und Anwendungen. Es gibt allerdings Lösungen und Methoden für einen sicheren und zuverlässigen Betrieb hybrider Cloudlandschaften. Im Wesentlichen gelingt dies mit einer sorgfältigen Planung und wohldurchdachten Hardware- und Software-Investitionen.



Grundlagen: Die eigene IT kennen

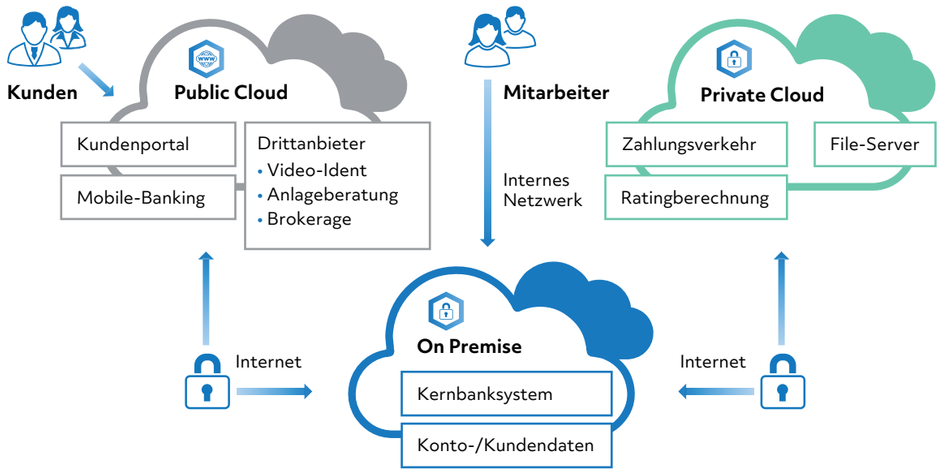
Bei einer Hybrid Cloud werden bestimmte Services bei öffentlichen Anbietern über das Internet betrieben, die Verarbeitung datenschutzkritischer Anwendungen und Daten dagegen im Unternehmen mittels On-Premise- respektive Private-Cloud-Lösungen vorgenommen.

Dafür ist es wichtig, die eigenen Geschäftsprozesse genau zu analysieren und in solche mit kritischen oder eben mit weniger kritischen Daten einzuteilen. Ohne eine dezidierte IT-Landkarte ist das schwer zu handhaben.

Die Klassifizierung bestimmt den Sicherheitsbedarf

Datenschutzregulierungen legen fest, wie und wo Banken Kundendaten erheben und speichern dürfen. Sind in einem Prozess personenbezogene oder geschäftskritische Daten involviert, ist die erste Wahl für die Verarbeitung On-Premise oder die Private Cloud. Sofern eine Hybrid Cloud genutzt werden soll, besteht für Banken das Risiko, dass personenbezogene oder andere kritische Daten in der bei einer Mischlösung involvierten Public Cloud falsch behandelt werden. Schlimmstenfalls gelangen sie sogar ins EU-Ausland, obwohl die DSGVO vorschreibt, dass Daten von EU-Bürgern nur innerhalb der EU lagern dürfen. Entsprechend wichtig ist es, von Anfang an zu verhindern, dass sensible Daten nach Außen dringen.

Hybrid Cloud – Funktionsschema



Eine Hybrid Cloud bietet die notwendige Datensicherheit, ohne unnötige Zugangshürden aufzubauen.Bei flexibler Handhabung können dadurch auch sehr sensible Vorgänge in die Cloud verlagert werden.

Datensicherheit gewährleisten

Bei der Nutzung der Cloud ist Verschlüsselung Pflicht! Das betrifft nicht nur die die Ablage der Daten, sondern auch ihre Transferwege. Allerdings löst eine Verschlüsselung des Datenverkehrs allein noch nicht alle IT-Sicherheitsprobleme. Auch ein übergreifendes Identitätsmanagement ist einer Mischform aus Cloud- und lokalen Diensten von immenser Bedeutung. Für die Dokumentation der Datenintegrität sind neben den lokalen Zugriffen und digitalen Identitäten auch diejenigen aus der Cloud einzubeziehen.

Datenredundanz sicherstellen

Zur Vermeidung von Ausfällen bei sensiblen und kritischen Daten kommen Hochverfügbarkeitscluster oder Datenspiegelungen in Betracht, auch in der Cloud. Zusätzlich ist ein umfassendes Backup-Konzept wichtig. Um beispielsweise das 3-2-1 Prinzip, also drei Kopien auf zwei verschiedenen Speichermedien sowie eine externe Sicherung zu erfüllen kann Letztere zur räumlichen Trennung verschlüsselt in der Cloud erfolgen. Das reduziert das Risiko eines vollständigen Datenverlusts.

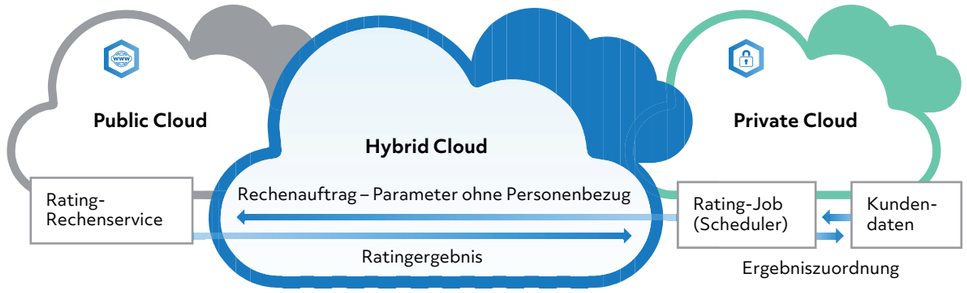
Hybrid in der Praxis: Verteilte Lasten

Mit einer hybriden Cloud lassen sich Lastschwankungen gut abfedern. Eine optimale Lastverteilung schafft mehr Ausfallsicherheit und spart Kosten.

Das Beispiel einer Ratingberechnung zeigt, wie dies datenschutzkonform gelingen kann: Vor einer Kreditzusage unterzieht so gut wie jede Bank den Kunden einem Online-Rating. Da in die Ermittlung des Ratings viele personenbezogene Daten einfließen, nutzt das Institut aus Sicherheitsgründen eine Private Cloud. Zusätzlich muss die Bank aber für die Ermittlung der Eigenkapitalquote die Kunden regelmäßig einem Bestandsrating unterziehen. Dazu werden einmal im Monat alle Kunden in einem Batchverfahren erneut einer Ratingermittlung unterzogen. Bei einer Großbank können dies viele Millionen Kunden sein. Für eine solche einmalige Lastspitze wurde die Private Cloud aus Kostengründen aber nicht ausgelegt. Stattdessen bucht das Finanzinstitut für diese Lastspitze zusätzliche Kapazitäten einer Public Cloud hinzu.

Aus Datenschutzgründen wird die eigentliche Ratingberechnung als vollkommen autarker Rechenkern aus der Ratingermittlung herausgelöst und als autarker Service in einer Public Cloud angelegt. Dort wird dann auf der Basis vieler Eingangsparameter die Ratingnote berechnet. Vorher werden aus diesen Variablen sämtliche Personenbezüge entfernt. Das Ergebnis wird in die Private Cloud zurückgespielt und dort mit der Person wieder in Beziehung gesetzt. Auf diese Weise muss die Private Cloud nicht für wenige Ereignisse im Jahr unnötig groß dimensioniert werden.

Ratingberechnung in der Hybrid Cloud



Um für eine Ratingberechnung die Public Cloud nutzen zu können, müssen die übertragenen Daten komplett anonym sein. Erst in der Private Cloud werden die berechneten Ergebnisse wieder mit den Kundenstammdaten verbunden.

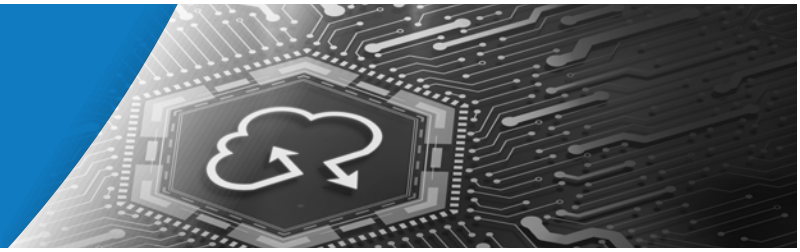
Übergreifendes Management gefragt

Eine hybride Cloudumgebung kann zu einem großen Netzwerk mit vielen verschiedenen Verbindungspunkten anwachsen. Die Kombination aus On-Premise-Systemen mit der Public und Private Cloud großer Anbieter wie Amazon oder Microsoft macht ein übergreifendes Management unerlässlich. Dazu können verschiedene, miteinander zu verknüpfende Tools zum Einsatz kommen, die administriert und aufeinander abgestimmt werden müssen. Dazu gehören beispielsweise ein übergreifendes internes Kontrollsystem (IKS) zur Protokollierung und zum Monitoring der gesteckten Ziele sowie das bereits oben erwähnte Identitätsmanagement zur Verwaltung der digitalen Identitäten und Zugriffe.

Hybridlösungen mit der PPI AG

Eine Hybrid Cloud kann Finanzdienstleisten erhebliche Vorteile bringen. Nicht umsonst setzen viele Unternehmen weltweit auf solche Cloudarchitekturen oder planen deren Einsatz. Gleichwohl ist eine Hybridlösung immer auch mit großen Hürden verbunden, die es zu meistern gilt. Die PPI AG verbindet ihre langjährige Erfahrung und bankfachliche Expertise mit der technischen Kompetenz zu Cloudthemen, um Finanzinstituten den Übergang in die Cloud so einfach wie möglich zu machen.

ppi



Bei Fragen und für weitere Informationen:

Frank Lohmeier
Partner
+49 151 57 13 23 31
frank.lohmeier@ppi.de

Thomas Diehl
Senior Consultant
+49 170 79 37 745
thomas.diehl@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
Germany