WHITE PAPER

Operative Resilienz in der Cloud

Warum führende Finanzdienstleister und Aufsichtsbehörden besorgt sind und was Sie dagegen tun können.

Graham Corr, Leitender Industrie-Consultant,
EMEA Financial Services Practice

teradata.

Inhaltsverzeichnis

Daten als Herzstück der operativen Resilienz

Es ist 7 Uhr morgens und der Arbeitstag hat gerade erst begonnen, als Ihr Cloud-Anbieter seine Statusseite aktualisiert, um einen Stromausfall in einem Rechenzentrum zu melden. Wird sie sich auf Ihre Dienste auswirken – auf welche und wie lange? Können Sie kritische Betriebsabläufe aufrechterhalten – und was sind die Folgen, wenn Sie es nicht können?

Es ist unmöglich, vorherzusagen, wie und wo der nächste Ausfall eintreten wird, oder sich auf alle Eventualitäten vorzubereiten. Operative Resilienz in einer vernetzten, Cloud-basierten Welt ist die Herausforderung, die Führungskräfte im Finanzdienstleistungssektor und Aufsichtsbehörden nachts wach hält. Die starke Abhängigkeit von einer Handvoll globaler Anbieter führt zu neuen systemischen Risiken in diesem Sektor. Es besteht Handlungsbedarf, und die Zeit zum Handeln ist jetzt gekommen.

Die Verlagerung von Anwendungen und Abläufen in die Cloud bedeutet nicht, dass eine betriebliche Ausfallsicherheit bereits „eingebaut“ ist. Die Abhängigkeit von Single-Cloud- oder „Cloud-only“-Implementierungen birgt das Risiko erheblicher Unterbrechungen, wenn ein Anbieter ausfällt. Und wie die jüngsten Ereignisse gezeigt haben, kann es selbst bei den größten Cloud-Anbietern aus verschiedenen Gründen zu Ausfällen kommen. Unabhängige Experten verzeichneten im Jahr 2020 21 separate Ausfälle von großen Cloud-Plattformen, und auch im Jahr 2021 kam es bei AWS, Microsoft, Google und Facebook zu ernsthaften Ausfällen.

Finanzdienstleistungsunternehmen müssen in ihre eigene betriebliche Ausfallsicherheit investieren, um unerwartete plötzliche Ausfälle aufzufangen und schnell zu reagieren, damit der Betrieb unter allen Umständen aufrechterhalten werden kann.

Operative Resilienz muss ein detailliertes Bewusstsein für die Risiken des Datenflusses im gesamten Unternehmen und präzise Pläne für den Zugriff, die Wiederherstellung und die fortgesetzte Nutzung von Daten beinhalten, um die kontinuierliche Einsatzfähigkeit kritischer Funktionen zu unterstützen.

Aufsichtsbehörden verlangen zunehmend einen Nachweis für Ausfallsicherheit, denn die Kosten, die entstehen, wenn wichtige Unternehmensdienste nicht mehr erbracht werden können, könnten katastrophale Folgen haben. Die Sicherstellung des kontinuierlichen Zugriffs auf kritische Daten muss einer der wichtigsten Punkte in jedem Plan für betriebliche Ausfallsicherheit sein.

teradata.

Verstehen der operativen Resilienz in der neuen Cloud-Landschaft

Die Cloud bietet viele Möglichkeiten und Vorteile für Finanzdienstleistungsunternehmen. Dementsprechend verlagern immer mehr Unternehmen zunehmend ihre Arbeitslasten in die Cloud.

- Zwischen 40 % und 90 % der Arbeitslasten von Banken weltweit könnten innerhalb eines Jahrzehnts in einer Public Cloud oder als Software-as-a-Service gehostet werden.[1]

Die Effizienz und die Kosteneinsparungen durch die Cloud liegen auf der Hand. Ein Cloud-zentrierter Betrieb bringt jedoch neue Risiken mit sich und stellt diejenigen, die für die Aufrechterhaltung der betrieblichen Ausfallsicherheit zuständig sind, vor andere Herausforderungen. Die Verwaltung von Daten und Workloads in der Cloud erfordert ein gewisses Maß an Kontrolle im Austausch gegen Flexibilität und Kosteneinsparungen. Es muss umfassend geprüft werden, was diese Kompromisse für die operative Resilienz bedeuten; „Cloud-first"-Strategien sollten nicht zu „Cloud-only"-Strategien werden, ohne diese neuen Risiken eingehend zu untersuchen.

Kommerzielle Risiken der Cloud

Der Wechsel in die Cloud bedeutet, dass Sie mit neuen Partnern zusammenarbeiten und ihnen Ihre Daten anvertrauen müssen. Ein vollständiges und umfassendes Verständnis der Bedingungen, die diese Beziehungen regeln, ist für die Aufrechterhaltung der operativen Resilienz unerlässlich. Wie einfach ist es, Daten von Cloud-Partnern bei Bedarf zu repatriieren? Was wird es kosten?

Finanzdienstleister müssen auch die Auswirkungen der von Cloud-Service-Anbietern (CSPs) auferlegten Bedingungen auf die operative Resilienz bewerten.

- Weltweit werden fast zwei Drittel aller Cloud Services (61 %) von den drei führenden CSPs der Big Tech (Amazon, Microsoft und Google) bereitgestellt.[2]
- 70 % der Banken und 80 % der Versicherer verlassen sich auf nur zwei Cloud-Anbieter für IaaS (Infrastructure as a Service).[3]

Dieser Zusammenschluss verleiht Big Tech erhebliche Macht bei der Festlegung der Bedingungen und der Definition der Art der Geschäftsbeziehungen. Sind ihre Bedingungen mit der internen Governance und Compliance vereinbar, stehen sie im Einklang mit den Plänen für betriebliche Ausfallsicherheit? Verfügt das Unternehmen über die Flexibilität, die es braucht, um widerstandsfähig zu sein, oder ist es an einen einzigen Lieferanten gebunden, der die Geschäftsbedingungen diktieren kann?

> **„Diese geballte Macht in Bezug auf die Bedingungen kann sich in Form von Geheimniskrämerei und Undurchsichtigkeit äußern und dazu führen, dass den Kunden nicht die Informationen zur Verfügung gestellt werden, die sie benötigen, um das Risiko des Dienstes zu überwachen.**
>
> Andrew Bailey, Gouverneur der Bank of England[4]

Kommerzielle Aspekte der operativen Resilienz sollten auch den Datenschutz und die Gefährdung durch Cyber-Risiken berücksichtigen. Obwohl die Anbieter von Cloud Services erhebliche Investitionen in den Datenschutz und die Cybersicherheit getätigt haben, ist niemand vor Angriffen gefeit.

Darüber hinaus muss die Einhaltung der Datenschutz-Grundverordnung (DSGVO) und ähnlicher Schutzmaßnahmen für personenbezogene Daten als zentrales Element der betrieblichen Widerstandsfähigkeit beibehalten werden. Es ist von entscheidender Bedeutung, genau zu wissen, wo die Daten gespeichert sind, und nachweisen zu können, dass jede Datenübermittlung mit den lokalen Gesetzen in Einklang steht. Dies gilt auch für den Wechsel zu und zwischen Anbietern von Cloud Services.

1 https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report

2 https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

3 https://www.imf.org/en/News/Articles/2021/06/16/sp061721-bigtech-in-financial-services

4 https://www.reuters.com/business/retail-consumer/bank-england-crack-down-secretive-cloud-computing-services-2021-07-13

teradata.

Das Urteil des Gerichtshofs der Europäischen Union (EuGH) in der Rechtssache Schrems II beispielsweise legt den Unternehmen eindeutig die Verantwortung auf, ein zusätzliches Schutzniveau für personenbezogene Daten zu gewährleisten, wenn dies von den Cloud-Anbietern nicht garantiert werden kann.[5]

Risiken von Cloud-Technologie

Finanzinstitute, die an wöchentliche Failover-Tests von Rechenzentren vor Ort gewöhnt sind, müssen möglicherweise bald ähnliche Ausfallsicherheitstests für Cloud-basierte Infrastrukturen in Betracht ziehen. Im Großbritannien beispielsweise sucht die Aufsichtsbehörde Prudential Regulation Authority nach Möglichkeiten, mehr Informationen von großen Cloud-Anbietern zu erhalten, um das Risiko von technischen Ausfällen von Cloud Services besser einschätzen zu können.[6]

Nach Berichten der Financial Times sagte eine mit den Plänen der Aufsichtsbehörde vertraute Person: „Wir betrachten Cloud-Anbieter unter dem Gesichtspunkt der betrieblichen Ausfallsicherheit bzw. operativen Resilienz. Müssen wir mehr eingreifen, wie können wir ihnen Vertrauen entgegenbringen? Wir fangen an, sie als kritische Dritte zu betrachten, die wir stärker beaufsichtigen müssen“.[6]

Hybride und Multi-Cloud-Strategien sind auf dem Vormarsch, um das Risiko von Single Points of Failure und die Bindung an einen bestimmten Anbieter zu verringern.

- Die eigenen Untersuchungen von Google Cloud zeigen, dass 28 % der Finanzdienstleistungen derzeit von einem einzigen Anbieter abhängig sind.
- Aber 88 % derjenigen, die Multi-Cloud noch nicht nutzen, ziehen es in Betracht.[7]

Bei der Betrachtung der technischen Hindernisse für die betriebliche Ausfallsicherheit müssen die Lock-in-Risiken sowie die Einfachheit der Replizierung bestimmter Arbeitslasten in verschiedenen Clouds bewertet werden. Auch die Möglichkeit der Rückführung in eine eigene On-Premise-Infrastruktur muss berücksichtigt werden.

Systemische Risiken der Cloud

Die Aufsichtsbehörden sind besorgt, dass die systemischen Risiken zunehmen, da der Anteil der von der Cloud abhängigen Dienste steigt.

- Fast die Hälfte der Workloads im Finanzdienstleistungsbereich werden heute in Public Clouds ausgeführt.[8]
- „Die zunehmende Abhängigkeit von einer kleinen Anzahl von CSPs und anderen kritischen Dritten könnte die Risiken für die Finanzstabilität erhöhen, wenn nicht eine stärkere direkte regulatorische Aufsicht über die Widerstandsfähigkeit der von ihnen erbrachten Dienste erfolgt.“ Die Bank of England, Juli 2021.[9]

5 https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022

6 https://www.ft.com/content/29405a47-586b-4c5a-b641-0f479b4cee1d

7 https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services

8 https://www.statista.com/statistics/1257930/cloud-workloads-financial-services-banking

9 https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management

teradata.

Was die Aufsichtsbehörden tun

Aufsichtsbehörden auf der ganzen Welt haben bereits damit begonnen, auf diese Risiken zu reagieren.

In Großbritannien zum Beispiel, einem der ersten Länder, das Maßnahmen ergriffen hat, wurden im März 2021 neue Vorschriften für die operative Resilienz eingeführt. Den Finanzinstituten wurde nur ein Jahr für die Umsetzung eingeräumt, und die knappen Fristen verlangen von den Unternehmen, dass sie ihre Fähigkeit, ihre Toleranzgrenzen für die Auswirkungen einzuhalten, vollständig nachweisen. Die Aufsichtsbehörde ging sogar so weit, dass sie in ihren im März 2021 herausgegebenen Grundsatz- und Aufsichtserklärungen (PS7/21 und SS2/21) sowohl IKT-Outsourcer als auch die Gefahren des Konzentrationsrisikos ausdrücklich erwähnte. Der besondere Schwerpunkt dieser Erklärungen lag auf dem Management der Ausfallsicherheit in einer Cloud-first-Umgebung.

Sie betonen, wie wichtig es ist, eine übermäßige Abhängigkeit von einem einzigen Anbieter ausgelagerter IKT (einschließlich Cloud Services) zu vermeiden und die Ersetzbarkeit von Cloud Services zu gewährleisten (einschließlich der Ermittlung geeigneter alternativer Anbieter). Sie fordern auch Nachweise über geplante vorübergehende Maßnahmen zur Fortführung des Betriebs im Falle eines Ausstiegs des Unternehmens aus irgendeinem Grund.

Bis zum Ende des Übergangszeitraums im März 2025 müssen die Unternehmen in der Lage sein, nachzuweisen, wie die betriebliche Ausfallsicherheit für alle Anlagen (einschließlich Daten und Technologie), die mit der Erbringung wichtiger Geschäftsdienstleistungen verbunden sind, aufrechterhalten werden kann. Die PRA erklärt, dass sie ***„von den Unternehmen erwartet, dass sie die Anforderungen an die Ausfallsicherheit der auszulagernden Dienste und Daten bewerten und sich auf der Grundlage eines risikobasierten Ansatzes für eine oder mehrere verfügbare Cloud-Ausfallsicherheitsoptionen entscheiden.“***

In Europa, das ebenfalls frühzeitig Maßnahmen ergriffen hat, gibt es einen etwas anderen Ansatz. Der Digital Operational Resilience Act, bekannt als DORA, zielt auf viele der gleichen Risiken ab und ist ein Grundpfeiler des umfassenderen europäischen Gesetzes über die digitale Finanzierung (European Digital Finance Act). Die Verordnung umreißt nicht nur die Anforderungen an die digitale Widerstandsfähigkeit von Unternehmen, einschließlich der Forderung nach Strategien für IKT mit mehreren Anbietern und der Erfassung technologischer Abhängigkeiten, sondern geht auch weiter als andere Verordnungen, indem sie die Aufsicht auf wichtige Drittanbieter ausdehnt.

Dazu gehören ausdrücklich auch Anbieter von Cloud Services. Je nach Umfang, Komplexität und Bedeutung müssen die Unternehmen ein Verzeichnis aller vertraglichen Vereinbarungen führen, die von IKT-Drittanbietern getroffen wurden. Die Anbieter selbst werden einer behördlichen Aufsicht unterliegen, um sicherzustellen, dass sie über Pläne und Verfahren verfügen, die die Unternehmen vor technologischen Risiken schützen.

Aufgrund der Komplexität dieser Gesetzgebung könnten sich die Fristen verlängern. Jedoch wurde der erste DORA-Entwurf bereits im September 2020 veröffentlicht und ein endgültiger Entwurf wird für 2022 erwartet, wobei das Europäische Parlament, der Rat und die Kommission im Trilog darüber beraten sollen. Mit der Durchsetzung wird ein Jahr nach Verabschiedung des Gesetzes gerechnet. Parallel dazu sollen in Kürze weitere Verbesserungen und Erweiterungen (Stufe 2) veröffentlicht werden, die 2 bis 3 Jahre später zur Diskussion und Einigung stehen. Sie wird erhebliche Auswirkungen auf die Art und Weise haben, wie europäische Finanzinstitute ihre Cloud-Service-Anbieter unter Vertrag nehmen und verwalten, und es wird ihnen empfohlen, jetzt mit der Planung zu beginnen.

Die Aufsichtsbehörden Großbritanniens und der EU haben bisher die fortschrittlichsten Maßnahmen für die operative Resilienz ergriffen. Andere Gerichtsbarkeiten auf der ganzen Welt, darunter auch die USA, beginnen jedoch mit der Umsetzung ähnlicher Maßnahmen. Unternehmen müssen die lokalen Vorschriften für die operative Resilienz in den Märkten, in denen sie tätig sind, befolgen. Jedoch gibt es Anzeichen dafür, dass die Vorschriften in diesem Bereich nur noch zunehmen werden.

teradata.

Die Beantwortung der schwierigen Fragen jetzt ist wirtschaftlich sinnvoll

Der rote Faden, der all diese Regulierungsmaßnahmen miteinander verbindet, ist die Notwendigkeit für Unternehmen, ihre operative Resilienz angesichts eines plötzlichen, ungeplanten Ausstiegs aus einem Cloud Service (Stressed Exit) zu beweisen. Die Aufsichtsbehörden werden detaillierte Pläne verlangen, deren Wirksamkeit durch strenge Tests nachgewiesen werden muss. Veröffentlichte Vorschriften und Regulierungsvorschläge der PRA[10], der EZB[11] und der Federal Reserve[12] deuten alle auf weitere Tests in diesem Bereich hin. Finanzinstitute können sich jedoch auf diese Anforderungen vorbereiten und gleichzeitig die skalierbaren, schnellen und flexiblen Datenplattformen aufbauen, die sie benötigen, um in der digitalen Welt wettbewerbsfähig zu sein.

Die Aufsichtsbehörde wird die Cloud-Strategien der Unternehmen und ihre Fähigkeit, mit plötzlichen unerwarteten Ausfällen umzugehen, genau unter die Lupe nehmen – von Cloud-Ausfällen bis hin zu vertraglichen Unstimmigkeiten und Geschäftsausfällen von Lieferanten. Aus der Datenperspektive werden sie Pläne für den Zugriff auf und die Nutzung von Daten aus dem gesamten Unternehmen testen wollen, um die Analysen und die automatisierte Entscheidungsfindung auch während eines längeren Ausfalls eines Cloud-Anbieters zu unterstützen.

Zu wissen, wo sich die Daten befinden, welche wichtigen Geschäftsdienste auf welche Datensätze darauf angewiesen sind und wo wichtige Analytics-Modelle laufen, ist der erste grundlegende Schritt zum Aufbau dieser Resilienz. Führende Organisationen sind bei der Beantwortung dieser Fragen bereits weit fortgeschritten. Der ungehinderte Fluss von Daten im gesamten Unternehmen, damit sie auf innovative Weise für die Entwicklung neuer Dienste und die Verbesserung der Kundenerfahrung genutzt werden können, ist der Kern der digitalen Transformation der Branche. So gesehen sind die Forderungen der Aufsichtsbehörde, operative Resilienz nachzuweisen, ein zusätzlicher Nutzen, der aus diesen laufenden Projekten gezogen werden kann.

Anstatt die verstärkte Kontrolle durch die Aufsichtsbehörden und die Notwendigkeit, die operative Resilienz zu entwickeln, um den Verlust von „too big to fail"-Cloud-Service-Anbietern zu verkraften, als separate und lästige Aufgabe zu betrachten, können Unternehmen diese Anforderungen als zusätzliche Wegweiser zu effektiven Dateninfrastrukturen integrieren.

Checkliste für die operative Resilienz

Daten und Data Analytics müssen in Ihren Plänen für operative Resilienz umfassend berücksichtigt werden. Haben Sie sich diese Fragen gestellt und sind Sie mit den Antworten zufrieden, die Sie erhalten haben?

- Haben Sie mit Ihren Cloud-Anbietern Ausstiegspläne besprochen?
- Bieten sie konforme Vertragsklauseln, die den „Stressed Exit" erleichtern?
- Haben Sie die Sicherheits-, Heilungs- und Wiederherstellungszusagen der CSPs überprüft?
- Wissen Sie, wo alle Ihre Daten sind?
- Haben Sie eine Analyse zur Arbeitslastverteilung durchgeführt?
- Können Sie Datenabhängigkeiten von wichtigen Geschäftsdiensten abbilden?
- Können Sie alle Workloads für Data Analytics identifizieren, die für wichtige Geschäftsdienste unerlässlich sind, und wissen Sie, wo sie laufen?
- Wie schnell können Sie Analytics-Modelle auf alternativen Plattformen replizieren?

10 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B41473OC697DC8BEB353F3EE5A628

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-_en

12 https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

teradata.

Was Sie jetzt tun müssen

Viele Finanzinstitute haben sich bereits für Multi-Cloud-Ansätze entschieden. Ob aus finanziellen oder betrieblichen Gründen oder um bestimmte Arbeitslasten mit bestimmten technologischen Merkmalen in Einklang zu bringen – ein Multi-Cloud-Ansatz bietet die Grundlage für operative Resilienz. Allerdings bieten Multi-Cloud-Architekturen für sich genommen möglicherweise nicht ausreichend Ausfallsicherheit. Möglicherweise gibt es noch immer technische, finanzielle und vertragliche Hindernisse, die es erschweren, Arbeitslasten aus einer Cloud in eine andere zu verlagern.

Die Hinzufügung (oder Beibehaltung) von On-Premise-Infrastruktur kann eine weitere Ebene der Ausfallsicherheit schaffen. Die Beibehaltung der Möglichkeit, kritische Dienste über eine eigene Infrastruktur unter direkter Kontrolle der Bank zu erbringen, kann als Puffer dienen, falls Cloud-basierte Ressourcen aus irgendeinem Grund unzugänglich werden.

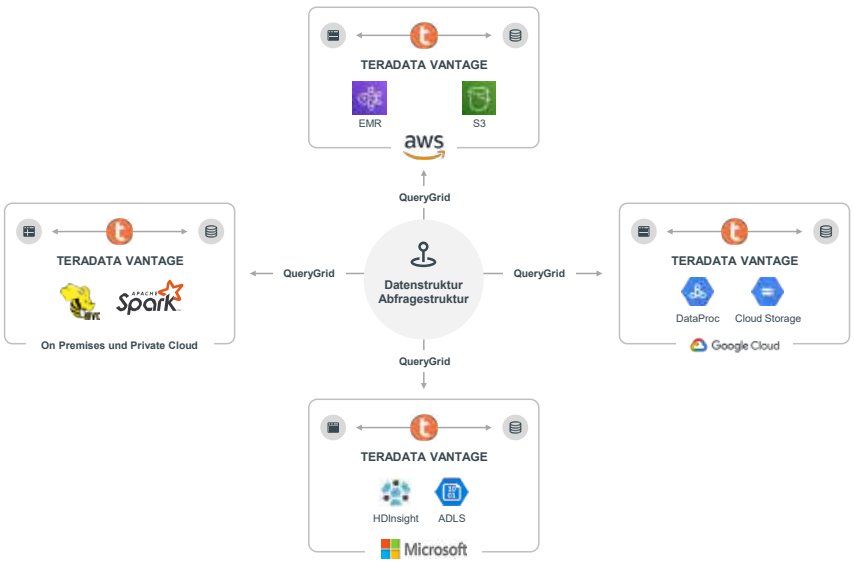
Die Kombination der beiden Ansätze mit einer vernetzten Cloud-Datenumgebung bietet eine Lösung. Die Schaffung einer Datenplattform, die nahtlos mit Clouds beliebiger Anbieter sowie mit On-Premise-Lösungen zusammenarbeitet, bietet nicht nur betriebliche Ausfallsicherheit bzw. operative Resilienz, sondern auch Flexibilität, um die Ziele der digitalen Transformation kosteneffizient zu verfolgen. Eine solche Lösung kann Daten aus beliebigen Anwendungen verbinden und synchronisieren und den Datenbedarf des Unternehmens vom grundlegenden Data Warehousing bis hin zu fortgeschrittenen Analytics unterstützen.

So könnte es aussehen

Organisationen auf der ganzen Welt nutzen die Leistung und multidimensionale Skalierbarkeit von Teradata, um unternehmensweite Cloud-Datenplattformen zu schaffen, die ihre sich entwickelnden Anforderungen für Analytics zukunftssicher machen. Teradata fungiert als Single Point of Truth, der Daten aus beliebigen Quellen integriert, und stellt sicher, dass die Daten dorthin fließen, wo sie benötigt werden. Wie das nachstehende Diagramm zeigt, können sie sich mit jedem beliebigen Cloud-Service-Anbieter verbinden, ohne auf die On-Premise-Funktionen verzichten zu müssen. Dies bietet nicht nur die Flexibilität, sich Optionen für die digitale Transformation offen zu halten, sondern erfüllt als zusätzlichen Vorteil auch die Anforderungen an die operative Resilienz.

Operative Resilienz

Architektonischer Entwurf für den nahtlosen Wechsel zwischen mehreren Cloud-Anbietern und die On-Prem-Rückverlagerung an den Standort, um die Geschäftskontinuität zu gewährleisten. Die hybride Multi-Cloud-Datenplattform von Teradata erhöht Ihre Flexibilität und verhindert, dass Sie an einen einzigen Public-Cloud-Anbieter gebunden sind.



Auf technische Genauigkeit geprüft im Februar 2022

Die Hochgeschwindigkeits-Datenstruktur (Data Fabric) verbindet Workloads in einer hochgradig verteilten Umgebung.

Die Wahl des Einstiegspunkts ermöglicht es, Abfragen in großem Umfang auf jedem System in der Data Fabric zu starten, sowohl On-Premises als auch in mehreren Public-Cloud-Umgebungen.

Die Pushdown-Verarbeitung ermöglicht minimale Datenübertragungs- und Datenrückholkosten (sogenannte Egresskosten), indem Abfragen so nah wie möglich an den Daten ausgeführt werden.

teradata.

Eine hybride und Multi-Cloud-Welt

Finanzdienstleistungsunternehmen führen Cloud-Architekturen als Grundlage für flexible, kundenorientierte Geschäftsmodelle rasch ein. Sie tun dies, um die Kosten zu senken und ihnen die Flexibilität zu geben, nicht nur auf ein unbeständiges wirtschaftliches und kundenbezogenes Umfeld zu reagieren, sondern auch, um die nächsten Wellen des Wandels vorherzusehen und zu planen. Jedoch sind Clouds selbst nicht statisch. Im Rahmen ihrer Strategien müssen Finanzinstitute die mit Cloud-Infrastrukturen verbundenen Risiken für die betriebliche Ausfallsicherheit sorgfältig bewerten und kontinuierlich überwachen.

Es bestehen kommerzielle, technologische und systemische Risiken, und die Aufsichtsbehörden sind bereits besorgt. Wo Europa und Großbritannien vorangegangen sind, werden andere sicherlich folgen. Führende Unternehmen antizipieren bereits die unvermeidliche Regulierung und bereiten sich darauf vor – die Zeit zum Handeln ist jetzt gekommen.

Die mit der Cloud verbundenen operativen Risiken können durch hybride Multi-Cloud-Ansätze gemildert werden, die Flexibilität und Ausfallsicherheit bewahren.

Heute arbeitet Teradata mit Finanzinstituten auf der ganzen Welt zusammen, die ihre Cloud-Strategien um Aspekte zur betrieblichen Ausfallsicherheit ergänzen.

Der hybride Multi-Cloud-Ansatz von Teradata erhöht die operative Resilienz, da er die Flexibilität bietet, Daten und Arbeitslasten nahtlos zwischen den Clouds zu verschieben und bei Bedarf von jeder Cloud in eine lokale Infrastruktur zu wechseln. Es kann geplante oder unvorhergesehene Ausstiege aus einer bestimmten Cloud (Stressed Exit) unterstützen, und im Falle eines Ausfalls können die Daten schnell auf allen Systemen vor Ort oder in der Cloud wiederhergestellt werden, die nicht betroffen sind, so dass der Betrieb fast unmittelbar wieder aufgenommen werden kann.

Der hybride Multi-Cloud-Ansatz von Teradata ist für jedes Finanzdienstleistungsunternehmen, das in der schnelllebigen digitalen Welt erfolgreich sein will, sinnvoll. Die Kombination dieser Vorteile mit einer verbesserten operativen Resilienz hat viele Finanzdienstleister dazu veranlasst, sich an Teradata zu wenden, um ihre Risikominderungsstrategien zu planen und auszuführen.

Über Teradata

Teradata nutzt alle Daten zu jeder Zeit, so dass Sie alles, was Sie wollen, analysieren, überall einsetzen und aussagekräftige Analysen liefern können. Durch die Bereitstellung von Antworten auf die Komplexität, die Kosten und die Unzulänglichkeiten heutiger Analysemethoden verändert Teradata die Art und Weise, wie Unternehmen arbeiten und Menschen leben. Die Antworten finden Sie unter Teradata.com.

Autor

Graham Corr Leitender Industrie-Consultant, EMEA Financial Services Practice

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata.