T-SYSTEMS WHITEPAPER

# EIN PRAXISLEITFADEN FÜR DAS MANAGEMENT VON MULTI-CLOUD-UMGEBUNGEN

COMPUTERWORLD in Kooperation mit T · · Systems ·

# 1

## KAPITEL 1: DER SIEGESZUG VON MULTI-CLOUD

**Eine sorgfältig geplante Multi-Cloud-Strategie erhöht die Flexibilität und Agilität Ihres Unternehmens und hilft gleichzeitig dabei, Kosten zu sparen.**

Wenn es um Cloud Computing geht, ist oft von „der" Cloud die Rede, als sei sie nur eine einzelne, einfach zu steuernde Plattform. Doch für die meisten Unternehmen gestaltet sich das Thema deutlich komplexer. Beim Cloud Computing gibt es keine Patentlösung. Viele Unternehmen greifen daher zunehmend auf eine Kombination aus Private und Public Clouds für spezielle Workloads und Anwendungen zurück. Das führt oft dazu, dass Unternehmen im IaaS-, PaaS- und SaaS-Bereich mit unterschiedlichen Cloud-Anbietern arbeiten.

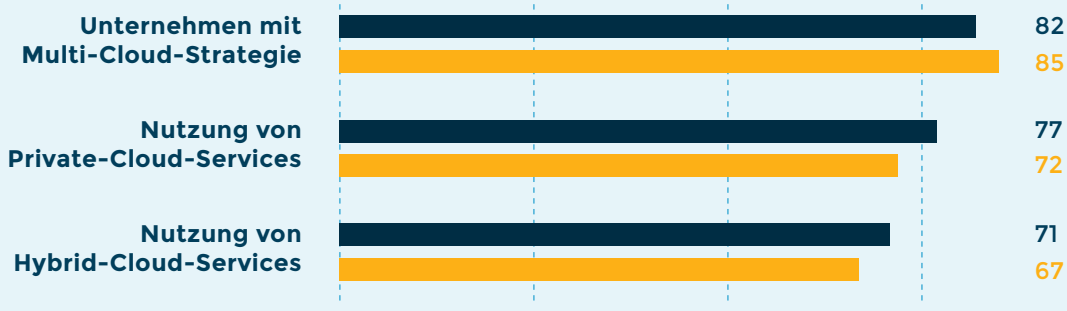
Unternehmen sind also nicht länger an die eigene verfügbare Technologie gebunden, sondern können die Cloud wählen, die sich am besten für die jeweilige Anforderung eignet. Beispielsweise wählt ein Unternehmen die SaaS-Plattform von Salesforce für das CRM, für den E-Mail-Verkehr MS Office, als Konferenzsystem WebEx und verschiedene IaaS-Anbieter für das Web-Hosting und die Nutzung von webbasierten Anwendungen.

Mit einer solchen Vorgehensweise, bei der Ressourcen jederzeit problemlos bereitgestellt und erweitert werden können, können Unternehmen ihre Flexibilität und Skalierbarkeit spürbar verbessern. Die Cloud ist dabei eine zusätzliche IT-Ressource, mit der sich bei Bedarf die Leistungsfähigkeit der IT steigern lässt und mit der die Kosten nutzungsbasiert abgerechnet werden.

In der Folge müssen Unternehmen Cloud-Services von einer Vielzahl von Partnern managen. Laut dem Cloud-Management-Spezialisten **RightScale** nutzen inzwischen vier von fünf Unternehmen Multi-Cloud-Services mit im Schnitt 3,6 verschiedenen Public Clouds und 4,4 Private Clouds. Das Analystenhaus IDC schätzt sogar, dass bis 2018 mehr als 85 Prozent der Unternehmen Multi-Cloud-Architekturen eingeführt haben werden.

**NUTZUNG VON CLOUD-SERVICES**
IN PROZENT

**Hybrid Cloud ist die bevorzugte Strategie in Unternehmen, jedoch ging die Nutzung von Private-Cloud-Services zurück, weshalb in der Folge auch die Nutzungszahlen für Hybrid Cloud sanken.**




QUELLE: RIGHTSCALE 2017 STATE OF THE CLOUD REPORT

## MULTI-CLOUD FÖRDERT DIE GESCHÄFTSKONTINUITÄT

Bei Multi-Cloud geht es einerseits darum, Workloads und Prozesse zu betreiben, für viele Unternehmen ist Multi-Cloud andererseits auch die perfekte Lösung, um Geschäftskontinuität sicherzustellen. Sie replizieren ihre Infrastruktur, Daten und Anwendungen in den Cloud-Umgebungen verschiedener Anbieter und können umgehend auf ein Backup zugreifen, sollte das Primärsystem ausfallen. Ausfallzeiten werden so deutlich reduziert. Eine geringere Anzahl an ungeplanten Ausfällen bedeutet wiederum, dass hohe Ausfallkosten vermieden werden können. Laut dem Analystenhaus **Ponemon Institute** verursachen ungeplante Ausfälle in Unternehmen Kosten in Höhe von 8.751 US-Dollar je Vorfall pro Minute.

**UNGEPLANTE AUSFÄLLE KOSTEN UNTERNEHMEN**
**8.751 DOLLAR**
**PRO VORFALL PRO MINUTE.**

Überdies kann die Verteilung von Anwendungen und Daten mithilfe von Cloud-Services kostengünstiger sein, als eigene Rechenzentren global vorzuhalten. Dabei kann es aus wirtschaftlicher Sicht und im Hinblick auf die Performance sinnvoll sein, Cloud-Services verschiedener Anbieter zu nutzen und diese nach Verbrauch abrechnen zu lassen, um die laufenden Kosten zu senken. Das setzt natürlich voraus, dass Dienste und Workloads sorgfältig gemanagt werden.

## MULTI-CLOUD WILL GUT DURCHDACHT SEIN

Multi-Cloud-Umgebungen bieten zwar zahlreiche Vorteile – für CIOs und deren IT-Teams birgt dies aber auch Risiken: Insbesondere für das Management mehrerer, verteilter Clouds bedarf es oft einer ganzen Reihe von Fähigkeiten. Im Besonderen benötigen Unternehmen geeignetes Fachpersonal, Fachkenntnisse, moderne Technologien und standardisierte Prozesse, um die Synergien von Multi-Cloud vollständig zu nutzen.

Einer der größten Vorteile ist es, Anwendungen, Daten und ganze Systeme jederzeit je nach Business-Anforderung zwischen verschiedenen Clouds migrieren zu können.  Die Herausforderung besteht aber gerade darin, die Migration einfach, sicher und schnell umzusetzen. Deshalb sollten Anwendungen, Plattformen und Infrastrukturen bereits so entwickelt und gemanagt werden, dass sie sich problemlos migrieren lassen.

Auch die Einhaltung von Governance-Vorgaben und Gesetzen kann bei Multi-Cloud-Umgebungen über mehrere Plattformen hinweg komplex sein. Besonders in Anbetracht der 2018 in Kraft tretenden Datenschutzgrundverordnung der EU (DSGVO) und der MiFID II, bei denen es um den Schutz und die Sicherheit von Daten geht. Darüber hinaus ist Cyber-Security eine weitere Herausforderung für alle Unternehmen.

**MEHR INFORMATIONEN FINDEN SIE IN KAPITEL 4**

Dennoch überwiegen die Vorteile von Multi-Cloud, wenn die Komplexität richtig gemanagt wird. Mit korrekt verwalteten SLAs, der Einhaltung von Governance- und Compliance-Regeln und der Wahl der richtigen Cloud für jede Anwendung werden Unternehmen agiler und senken gleichzeitig ihre Gesamtbetriebskosten (TCO).

„Wir sind der Überzeugung, dass eine Multi-Cloud-Strategie, die auf Mitarbeiter mit Verhandlungsgeschick, höhere Investitionen in Automatisierungssoftware und länderübergreifende Anbindungsmöglichkeiten setzt, ein Muss für IT-Abteilungen in innovativen Unternehmen ist", erklärt Giorgio Nebuloni, Leiter Research bei der IDC European Infrastructure Group, in einem **kürzlich veröffentlichten Bericht**.

Die meisten Unternehmen mit hohem Digitalisierungsgrad haben das bereits verstanden. So sichert der US-amerikanische Streaming-Riese Netflix seine auf AWS gehosteten Daten angeblich in der Google Cloud und über Apple wird **berichtet,** dass das Unternehmen mit drei IaaS-Anbietern arbeitet, um die Resilienz seines iCloud-Dienstes zu stärken.

Um die Komplexität des Betriebs verschiedener Clouds zu reduzieren, müssen Sie Ihre heterogene Infrastruktur zentral verwalten. Indem Sie dieses Management einem Provider überlassen, können Sie sich auf Ihr Kerngeschäft konzentrieren, Ressourcen besser bereitstellen und Ihre Unternehmens-IT effizienter steuern.

2

## KAPITEL 2: DIE RICHTIGE CLOUD FÜR JEDE ANWENDUNG

**Mit der richtigen Plattform für jeden Workload können Sie Ihre Dienste und Anwendungen optimieren und sich voll und ganz auf das Wachstum Ihres Geschäfts konzentrieren.**

Der entscheidende erste Schritt zu einer Multi-Cloud-Umgebung ist die Wahl eines geeigneten Cloud-Anbieters und der passenden Bereitstellungsform für alle Workloads und Anwendungen. Längst dreht sich die Diskussion auch in Europa nicht mehr um die „riskante" Public Cloud und die „sichere" Private Cloud. Vielmehr stehen der Business-Mehrwert und eine angemessene Risikoabschätzung bei der Diskussion um das Delivery-Modell der Cloud-Leistungen zu Recht im Vordergrund.

Der größtmögliche Mehrwert entsteht durch ein koordiniertes Zusammenspiel der einzelnen Modelle und durch die Wahl der am besten passenden Cloudplattform für jede Anwendung und jeden Workload.

## SO WÄHLEN SIE EINE PUBLIC CLOUD AUS

Üblicherweise werden Cloud-Services nutzungsbasiert abgerechnet, das heißt, Sie zahlen nur für die Ressourcen, die Sie auch tatsächlich nutzen. Das macht Public Cloud in vielen Fällen kosteneffizient und ermöglicht die Einschätzung der zukünftigen Kosten. Im Vergleich zur traditionellen Bereitstellung haben Public Clouds eine effizientere Auslastung, was sich im Energieverbrauch und der Auslastung zeigt. **McKinsey & Company** beispielsweise schätzt, dass ein klassischer Server pro Jahr nur etwa fünf bis 15 Prozent seiner maximal möglichen Rechenleistung erbringt.

General Electric (GE) ist ein Unternehmen, das den Wechsel in die Public Cloud bereits vollzogen hat. Rechenzentren wurden geschlossen und zusammengelegt und Anwendungen wurden, wo möglich, in die Public Cloud verlagert.

Bei der Migration sollten Firmen jedoch die richtige Balance finden, wie auch Chris Drumgoogle, COO der Global Operations CoreTech bei GE, betont. Denn auch wenn GE bereits Cloud-Services auf breiter Basis nutzt, gibt es dennoch Applikationen, die für eine Migration ungeeignet sind: Die meisten Anwendungen oder Systeme für den Bau oder Transport von Maschinen (beispielsweise Turbinen) sind „bei Weitem noch nicht bereit für die Cloud“, sagt Drumgoogle.

Andere Firmen verlagern einen großen Teil ihrer Daten und Anwendungen in die Cloud: Xero, ein Anbieter von Buchhaltungssoftware, migrierte etwa vor Kurzem 1,4 Petabyte an Daten, 3.000 Anwendungsserver und 120 Datenbanken in eine Public Cloud. „Wir erhoffen uns viele Vorteile von der Migration in die Public Cloud“, so Mark Rees, Geschäftsleiter für die Bereiche Plattform, Architektur und Bereitstellung bei Xero, im Gespräch mit der **Fortune**. Insbesondere wolle man durch die Migration neue Features schneller bereitstellen.

Doch auch wenn sich mithilfe von Cloud-Services die Wirtschaftlichkeit steigern und Kosten senken lassen, dürfen Themen wie Compliance, Haftung und Cyber-Sicherheit nicht vernachlässigt werden.

## SO WÄHLEN SIE EINE PRIVATE CLOUD AUS

Es gibt jedoch Business Anforderungen, die die Public Cloud nicht abdecken kann und für die eine Private Cloud die bessere Wahl ist. Private Cloud ist etwa die richtige Plattform für komplett gemanagte, geschäftskritische Produktivumgebungen oder wenn es um die Bereitstellung von IT-Infrastrukturen mit lokalen Anforderungen geht.

Private Cloud ermöglicht Unternehmen den sicheren und zuverlässigen Betrieb von großen Produktivumgebungen mit Business-Applikationen, die individuelle Anforderungen an Performance, Betrieb und Service

stellen. Der Bedarf an hochverfügbarer, ausfallsicherer Infrastruktur kann durch hohe SLAs für geschäftskritische Anwendungen im 24x7 Betrieb abgedeckt werden. Zudem können rechtliche Vorgaben oder Compliance-Regeln bezüglich der Datenhaltung den Betrieb in einer bestimmten geografischen Region oder auf dem Firmengelände eines Unternehmens zwingend erforderlich machen. In diesem Fall sollte individuell entschieden werden, ob das Unternehmen den Betrieb selbst managt oder an einen Provider übergibt.

Um die Leistungsfähigkeit und Produktivität der IT-Systeme am Frankfurter Flughafen zu steigern und die Betriebskosten kontinuierlich zu senken, beschloss die **Fraport AG** den Neubau ihres Rechenzentrums und übergab den Betrieb an T-Systems. Dadurch nutzt Fraport die Anbieter-Skaleneffekte für Einkauf, Wartung und Betrieb der Lösung und reduzierte bereits im ersten Jahr die Stückkosten um drei Prozent und den Energieverbrauch um 30 Prozent.

In einigen Fällen ist eine Public Cloud aufgrund ihrer Flexibilität die bevorzugte Wahl. Doch auch bei Private Clouds kann man Kapazitäten dank dynamischer Preismodelle kurzfristig anpassen. So lassen sich zum Beispiel Disaster-Recovery-Szenarien, bei denen die Daten der Applikationen nicht in der Public Cloud gespeichert werden dürfen, kosteneffizient umsetzen.

Es wäre schwer nachvollziehbar, wenn Unternehmen ausschließlich auf Private Cloud oder eine einzige Public Cloud setzen würden. Die Anforderungen an Applikationen und Daten sind zu spezifisch. Außerdem hat jede Cloud besondere Stärken und Schwächen, die sie für bestimmte Einsatzszenarien prädestinieren oder ausschließen.

## SICHERHEIT UND LEISTUNGSSTANDARDS

Die Sicherheit in der Public Cloud bereitet vielen Unternehmen Kopfzerbrechen. Dass Anwendungen und Daten extern gespeichert werden, widerspricht dem traditionellen, perimeterorientierten Sicherheitsdenken. Ab Mai 2018 müssen Public-Cloud-Anbieter allerdings den Anforderungen der EU-DSGVO entsprechen, die unter anderem vorsieht, Daten in Rechenzentren innerhalb der EU zu speichern.

Unternehmen haben jedoch weiterhin in keiner Public Cloud Kontrolle darüber, welche Hardware zum Einsatz kommt. Daher sind Service Level Agreements (SLAs) mit den Anbietern so wichtig: Darin vereinbaren Sie beispielsweise die benötigte Verfügbarkeit, insbesondere für geschäftskritische Anwendungen und Daten.

**Viele Unternehmen bevorzugen daher hybride oder Multi-Cloud-Umgebungen, in denen sowohl die drei Public-Cloud-Modelle (Software-as-a-Service, Platform-as-a-Service und Infrastructure-as-a-Service) als auch Private Cloud sowie On-Premise-Lösungen genutzt werden, um verschiedene Anwendungsfälle zu bedienen.**

- → **Die Private Cloud wird dabei typischerweise für geschäftskritische Anwendungen und Daten eingesetzt, bei denen es auf die absolute Kontrolle ankommt. Owens-Illinois, ein Fortune-500-Unternehmen, das Glasbehälter produziert, hat beispielsweise für seine technische Abteilung eine Private Cloud aufgesetzt. Mit den Services aus der Cloud will der Hersteller sein System zur Einhalten von Lieferterminen hochverfügbar halten.**
- → **Die Public Cloud hingegen bietet Skalierbarkeit und Flexibilität für andere Workloads und Anwendungen, etwa beim Hosting von E-Mail-Anwendungen und Produktivitätsanwendungen wie Office365.**

Auch die Geschwindigkeit beim Datenzugriff ist von Bedeutung, denn Anwendungen können beim Zugriff über das Internet langsamer scheinen als beim lokalen Betrieb. Ein schneller Internetzugang oder eine sichere Verbindung und eine verteilte Public Cloud mit Rechenzentren in der Nähe machen sich bei der Performance dann häufig positiv bemerkbar.

Wirklich flexibel sind Unternehmen meist dann, wenn sie verschiedene Bereitstellungsmodelle verwenden: für jede Anwendung und jeden Workload die am besten geeignete Cloud.

In einer solchen Multi-Cloud-Umgebung ist es wichtig, den passenden Provider für die unterschiedlichen Workloads auszuwählen, sowie Workloads und Jobs sicher, unkompliziert und schnell zwischen verschiedenen Cloud-Plattformen zu bewegen. Nur mit dem richtigen Partner an Ihrer Seite, der Ihnen bei der Auswahl und dem Management der Daten und der unterschiedlichen Cloud-Lösungen hilft, können Sie das Potenzial von Multi-Cloud voll ausschöpfen.

3

## DAS RICHTIGE VERHÄLTNIS ZWISCHEN ON-PREMISE- UND CLOUD-UMGEBUNGEN

**Das richtige Verhältnis zwischen On-Premise- und Multi-Cloud-Umgebungen erfordert eine sorgfältige Analyse und Überwachung von Workloads.**

Die Entscheidung darüber, welche Workloads in der Cloud und welche On-Premise betrieben werden sollten, ist nicht schwer – sie ist jedoch entscheidend für die Leistungsfähigkeit und den kosteneffizienten Betrieb von Anwendungen. Dieses Kapitel widmet sich daher der Frage, welche Kriterien bei der Auswahl beachtet werden sollten.

Ihre erste Frage lautet vermutlich: „Kann die Anwendung oder der Workload in der Public Cloud günstiger betrieben werden?“ Stellen Sie die Kosten für die Cloud-Migration den Kosten für die bestehende Infrastruktur, das Management und die Lizensierung gegenüber. Insbesondere klar definierte Anwendungen, die hinsichtlich ihrer Aufgaben und Nutzer abgegrenzt sind, können als SaaS-Variante kostengünstiger sein.

Die Gesamtkosten für Public Clouds lassen sich jedoch nur schwer bestimmen und viele CIOs befürchten, dass es zum Einsatz überflüssiger, kostspieliger Cloud-Anwendungen kommt. Doch zusammen mit einem Cloud-Management-Partner, der die Kosten transparent und damit steuerbar macht und die Cloud-Umgebungen managen kann, ist eine budgetgerechte Migration möglich.

**Doch wie bestimmen Sie die exakten Kosten für die Migration von Anwendungen in die Cloud? In einem Beitrag für Network World zeigt Mike Chan, CMO von Thorn Technologies, einem Spezialisten für Software-Entwicklung, einen Vier-Stufen-Plan auf, mit dem sich die Kosten für eine Cloud-Migration ermitteln lassen.**

**Diese vier Stufen sind:**

- → Prüfung der aktuellen IT-Infrastrukturkosten
- → Berechnung der voraussichtlichen Cloud-Infrastrukturkosten
- → Kostenschätzung für die Durchführung der Cloud-Migration
- → Gegenüberstellung von Kosten und Einsparungen nach der Migration – etwa durch höhere Verfügbarkeit

Anhand der Gesamtbetriebskosten (TCO) lässt sich bestimmen, welche Anwendungen und Workloads am meisten von einer Verlagerung in die Cloud profitieren. Wenn Sie alle Anwendungen in die richtige Cloud migrieren, können Sie signifikant Kosten senken. Das südafrikanische Unternehmen **Consol,** ein Hersteller von Glasbehältern, konnte durch den Wechsel in die Cloud von T-Systems in nur zwei Jahren 25 Prozent seiner Server-Betriebskosten einsparen, während gleichzeitig die Speicherkosten halbiert wurden.

Die Leistung jedes Workloads muss unbedingt bereits vor der Verlagerung in die Cloud überwacht werden. Sie müssen die durchschnittliche Leistung ebenso im Blick behalten wie Leistungsspitzen und -täler und wann diese auftreten. Diese Daten sind ein guter Anhaltspunkt, ob der entsprechende Workload in die Cloud gehört oder nicht. Können Sie beispielsweise einen Prozess, der nur periodisch läuft, beenden, wenn er nicht gebraucht wird? In diesem Fall ist eine Bereitstellung über eine Public Cloud möglicherweise die richtige Wahl, weil Sie für die Ressourcen nicht zahlen, wenn der Prozess nicht läuft.

MAPFRE, der größte Versicherer in Spanien, muss beispielsweise jeden Monat gemäß EU-Vorgaben eine Bonitätsprüfung vornehmen, für die eine sporadisch leistungsfähige Infrastruktur erforderlich ist.

**MIT DEM WECHSEL AUF EINE PUBLIC CLOUD KONNTE MAPFRE SEINE HARDWARE-INVESTITIONEN FÜR DIE KOMMENDEN DREI JAHRE VON 1,5 MIO EURO AUF 180.000 EURO SENKEN.**

## DER SIEGESZUG DES CLOUD-BURSTING

Prozesse mit Lastschwankungen sind ebenfalls gut in der Public Cloud aufgehoben, da die Ressourcen dynamisch erweitert oder reduziert werden können. Intern müssten andernfalls ausreichend Ressourcen für die Lastspitzen vorgehalten werden, die dann die meiste Zeit ungenutzt blieben. Eine solche Überdimensionierung ist ein gängiges Problem in Rechenzentren: **Computerworld** berichtet von einer Studie, nach der 20 bis 30 Prozent der Server „komatös" sind, das heißt sie verbrauchen Strom, ohne Informationen zu liefern.

Umgekehrt sind Prozesse mit stabilen Lasten meist besser und günstiger in einer Private Cloud aufgehoben. Solche Prozesse lassen sich einfacher bereitstellen und betreiben, so dass sich die Anschaffung der benötigten Ressourcen durchaus lohnen kann. Es wäre möglicherweise teurer, die gleichen Ressourcen aus einer Public Cloud zu beziehen.


In vielen Fällen muss eine Public Cloud auch gar nicht durchgängig genutzt werden. Stattdessen nutzt man „Cloud-Bursting". Dabei ist Ihre Private Cloud so ausgelegt, dass sie Ihre alltäglichen Anforderungen erfüllt. Kommt es nur einige wenige Male im Jahr vor, dass Sie zusätzliche Ressourcen benötigen, wäre es völlig unwirtschaftlich, Ihre IT-Infrastruktur an diesen Lastspitzen auszurichten.

Jacqui Taylor, CEO des Datenanalyse-Spezialisten Flying Binary, erklärt in ihrem Beitrag **„Bursting the IT legacy"** auf IDG Connect: „Ein Beispiel für einen Cloud-Service, bei dem das Cloud-Bursting in seiner ultimativen Form umgesetzt wird, ist eine Sendung, die nur Samstagabend für eine Stunde im britischen Fernsehen läuft und bei der die Zuschauer über den Gewinner abstimmen. Ein herkömmliches IT-System aufzusetzen, um ein Mal pro Woche für weniger als eine Stunde Zuschauerstimmen zu sammeln, wäre unwirtschaftlich. Eine PaaS-Lösung hingegen, die ausreichend Ressourcen genau für diesen Mehrbedarf zwischen 20 und 21 Uhr zur Verfügung stellt, lässt sich vergleichsweise günstig realisieren."

Damit diese Strategie aufgeht, braucht es – neben einer Cloud-Management-Plattform, die alles steuert – Anwendungen, die problemlos von einer Cloud in die andere verschoben werden können. Das lässt sich beispielsweise über skalierbare Microservices und Docker-Technologie verwirklichen.

## ALLES IM BLICK, ALLES IM GRIFF

Einige Workloads lassen sich aufgrund von Compliance-Vorgaben oder rechtlichen Vorgaben leichter in einer Private Cloud betreiben, weil Sie dort die volle Kontrolle über Datenzugriffe und den physischen Speicherort haben. Es kann außerdem sinnvoll sein, unterschiedliche Cloud-Plattformen für Daten und Anwendungen zu nutzen. Dabei sollten

Sie die gesetzlichen Vorgaben im Blick behalten, wie die EU-Datenschutzgrundverordnung (DSGVO), nach der die Daten von EU-Bürgen nur auf Servern innerhalb der EU (oder in von der EU genehmigten Ländern) gespeichert werden dürfen.

Jedes Unternehmen sollte wissen, welche Anwendungen und Daten besonders kritisch sind. Diese sind höchstwahrscheinlich am besten in einer Private Cloud aufgehoben, wo Sie eine bessere Kontrolle und einen besseren Überblick haben. Weniger kritische Anwendungen sollten, wenn möglich, in eine Public-Cloud- oder eine Hybrid-Cloud-Umgebung verlagert werden. Das spart Betriebskosten und setzt interne Ressourcen für den Ausbau geschäftskritischer Anwendungen oder für neue Projekte frei. Ein Provider, der die Verwaltung Ihrer Multi-Cloud-Umgebung übernimmt, ist dann möglicherweise die beste Lösung.

**UNTERNEHMEN SOLLTEN WISSEN, WELCHE ANWENDUNGEN UND DATEN BESONDERS KRITISCH SIND.**

Wo sollen die entsprechenden Anwendungen überall genutzt werden? Wenn sie in ganz Europa oder sogar weltweit ausgerollt werden sollen, kann es von Vorteil sein, Public Clouds in verschiedenen Regionen aufzusetzen. Insbesondere die Performance profitiert, wenn die Bereitstellung näher beim Nutzer erfolgt.

Im Artikel **„Eine Leitung reicht nicht“** erklärt T-Systems, dass internationale Unternehmen ihre Rechenzentren in der Regel über verschiedene Regionen verteilen. „Der Grund: Je weniger Strecke die Daten zurücklegen, desto kürzer dauert die Übertragung (Latenzzeit) und desto besser funktionieren besonders Echtzeit-Anwendungen.“

## 4 SICHERHEIT IN EINER MULTI-CLOUD-WELT

**Jede Plattform bringt gewisse Sicherheitsrisiken mit sich. Doch mit den richtigen Schutzmaßnahmen lassen sich die Risiken reduzieren und beherrschen.**

Vor dem Hintergrund der EU-DSGVO, die Einzelpersonen eine bessere Kontrolle über ihre eigenen Daten einräumt, nimmt die Relevanz des Themas Cyber-Sicherheit noch einmal zu. Unternehmen drohen Geldbußen in Höhe von bis zu 20 Mio. € oder 4 Prozent des weltweit erzielten Jahresumsatzes (je nachdem, welcher der Beträge höher ist), wenn sie den Datenschutzbestimmungen der EU-DSGVO zuwiderhandeln.

Mit einem soliden Sicherheitskonzept für Ihre Multi-Cloud-Umgebung tragen Sie zu einer höheren Datensicherheit bei und verringern die Gefahr von Datenverlust und -missbrauch. Ein wichtiger Schritt auf dem Weg zu einem solchen Konzept ist eine zuverlässige Cloud-Management-Lösung. Hier einige Aspekte, die Sie dabei berücksichtigen sollten:

Viele Clouds werden ad hoc aufgesetzt, mangelhaft konfigurierte Ressourcen bieten dann potenzielle Angriffsflächen für Cyber-Kriminelle. Mit der Erweiterung der Umgebung werden diese Fehler wiederholt und in neue Ressourcen und Cloud-Plattformen übernommen. Daher sollte jedes Unternehmen genau festlegen, wie die Cloud-Infrastruktur zu konfigurieren ist.


Im Artikel **„7 ways to take back control of your cloud strategy“** rät CSO Online: „Stellen Sie einen Ausschuss zusammen aus Vorstandsmitgliedern, Führungskräften der IT und Rechtsabteilung, Managern aus dem Bereich Compliance/Risikomanagement sowie Vertretern der Fachabteilungen. Lassen Sie diesen eine detaillierte Strategie zur Einführung von Cloud-Lösungen ausarbeiten, die auch die Themen Applikations-Auswahl und Sicherheitsrichtlinien umfasst, sowie Richtlinien für den Fall von Datenverlust, Notfallpläne und Metriken für das Reporting.“

**Schatten-IT**: Sind Daten und Anwendungen auf mehrere Cloud-Umgebungen verteilt, kann man schnell den Überblick verlieren. Laut **Shadow Data Report** von Blue Coat nutzen Unternehmen im Schnitt mehr als 840 Cloud-Anwendungen, und die meisten davon wurden ohne Wissen der IT-Abteilung eingeführt.

**Mehr Transparenz**: Den Überblick verschafft Ihnen Cloud-Management-Software: Damit sehen Sie, was Nutzer tun, welche Ressourcen aktuell zugewiesen sind und wer auf welche Daten zugreifen kann. Durch mehr Transparenz können Sie Gefahren und mögliche rechtliche oder Compliance-Probleme besser erkennen und Gegenmaßnahmen früher einleiten.

**Automatisches Monitoring**: Zusätzlich sollten automatisierte Überwachungssysteme eingerichtet werden, damit Probleme erkannt werden und Sie rechtzeitig darauf reagieren können. Solche Überwachungssysteme helfen auch, nicht genehmigte Cloud-Anwendungen zu finden.

## DIE BEDEUTUNG VON ZUGRIFFSKONTROLLEN

Sind mehrere Cloud-Umgebungen im Einsatz, teilt man schnell zu viele Daten mit zu vielen Personen – Zugriffskontrolle ist daher umso wichtiger. Michael Cooney erklärt in seinem **Artikel zur Zugriffskontrolle** auf Computerworld: „Über die Berechtigungskontrolle lässt sich das ‚Prinzip der minimalen Rechte' umsetzen, bei dem per Definition des amerikanischen National Institute of Standards and Technology Nutzern (oder von Nutzern gesteuerten Prozessen) nur die Zugriffsrechte eingeräumt werden, die sie für die Durchführung einer zugewiesenen Aufgabe in Übereinstimmung mit unternehmerischen Zielen und wirtschaftlichen Funktionen benötigen.“

Auch die Verbindung zwischen den einzelnen Cloud-Umgebungen einer Multi-Cloud sollte überwacht werden, damit bei einem Cyber-Angriff auf

ein System nicht zwangsläufig auch ein anderes betroffen ist. Ebenso sollten Sie prüfen, auf welche Systeme von anderen Unternehmen Sie zugreifen können und wer auf Ihre Systeme zugreifen kann: 2015 wurde die **US-Handelskette Target** Opfer von Hackern, die über einen Heizungs- und Klimatechnik-Dienstleister einen Weg in die Systeme gefunden hatten.

Häufig entscheiden sich Unternehmen für ein Modell, bei dem die Anwendungen in der Public Cloud gehostet werden, die dazugehörigen Daten aber (zumindest teilweise) in der Private Cloud liegen. Auf diese Weise lässt sich die Skalierbarkeit der Public Cloud mit der Sicherheit der Private Cloud kombinieren.

Mit dem Aufteilen Ihrer Daten entsprechen Sie auch den Anforderungen der Datenschutzgrundverordnung (DSGVO). An dieser Stelle kommt ein Verfahren zum Einsatz, das „Pseudonymisierung" genannt wird. Dabei werden personenbezogene Daten so verarbeitet, dass sie nicht ohne zusätzliche Informationen einer spezifischen Person zugeordnet werden können. Gemäß DSGVO müssen diese pseudonymisierten Daten getrennt von den zusätzlichen Informationen aufbewahrt werden. Dadurch können Cyber-Kriminelle aus gestohlenen Daten nur schwer Rückschlüsse auf die spezifische Person ziehen.

„Die DSGVO fördert die Datenmaskierung mit Zuckerbrot und Peitsche", erklärt Phil Lee, Anwalt im Team für Privacy, Security and Information bei der internationalen Anwaltskanzlei Fieldfisher, im Gespräch mit **Computerworld**.

„Pseudonymisierungsverfahren werden in der DSGVO als Teil guter Datenverarbeitung propagiert. Wer sie umsetzt, darf bei unvorhergesehenen Ereignissen wie sicherheitsrelevanten Zwischenfällen auf weniger bürokratischen Aufwand hoffen. Bei Unternehmen, die die Anforderungen der DSGVO nicht einhalten, schwingt der Gesetzgeber jedoch die Peitsche – in Form von Bußgeldern in Höhe von bis zu vier Prozent des weltweit erzielten Jahresumsatzes."

**„Die DSGVO fördert die Datenmaskierung mit Zuckerbrot und Peitsche."**

*Phil Lee Teil des Privacy, Security und Information Team bei Fieldfisher im Gespräch mit* **Computerworld**

Was also, wenn das Worst-Case-Szenario eintritt? Im Fall einer Datenschutzverletzung müssen Sie das Vorhandensein einer Richtlinie nachweisen, die auf Ihre Multi-Cloud-Infrastruktur abgestimmt ist. Diese sollte vorgeben, wie auf Datenschutzverletzungen zu reagieren ist, wie die Ausbreitung auf andere Cloud-Umgebungen verhindert wird und wie sich der Normalbetrieb wiederherstellen lässt. Solche Pläne sollten unbedingt gründlich getestet werden, damit sie im Bedarfsfall reibungslos funktionieren.

„Bei Datenschutzverletzungen ist es einfach ein Unterschied, ob man einen Notfallplan in der Schublade hat oder tatsächlich vorbereitet ist", zitiert **Computerworld** Michael Brummer, Vice President bei Experian Data Breach Resolution. „Leider gibt es diese Sicherheitsmaßnahme in vielen Unternehmen nur auf dem Papier. Ein Plan ist der erste Schritt, doch wirklich vorbereitet ist man nur, wenn der Plan im Sinne eines

kontinuierlichen Prozesses regelmäßig überarbeitet wird und Übungen durchgeführt werden." Damit Ihre Multi-Cloud-Umgebung geschützt ist, müssen entsprechende Sicherheitsmaßnahmen zu jedem Zeitpunkt greifen – von der Bereitstellung bis hin zum Zugriff.

## ZUSAMMENFASSUNG: OHNE MULTI-CLOUD GEHT ES NICHT

Im heutigen digitalen Zeitalter nutzen Unternehmen verschiedene Cloud-Services für ihre unterschiedlichen Workloads und Anwendungen. Das Ergebnis ist eine hybride Infrastruktur und Anwendungslandschaft, oft unübersichtlich und schwer zu verwalten. Das dafür erforderliche Know-how gehört meist nicht zu den Kernkompetenzen oder dem Geschäftsmodell des Unternehmens. Dabei erfordern gerade die Komplexität der Cloud-Umgebungen sowie ganz unterschiedliche Preismodelle, insbesondere bei Public Clouds, ein sicheres, zuverlässiges und kosteneffizientes Management. Keine leichte Aufgabe für IT-Abteilungen.

Vor diesem Hintergrund stellt Multi-Cloud eine Herausforderung dar – doch richtig eingesetzt können Unternehmen große Potenziale in Bezug auf Agilität und Reaktionsfähigkeit freisetzen.

**Sie möchten wissen, wie T-Systems das Management Ihrer Multi-Cloud-Umgebung vereinfachen kann und wie Cloud-Migration und -Optimierung zum Wachstum Ihres Unternehmens beitragen können? Dann schreiben Sie uns eine E-Mail und vereinbaren Sie ein Beratungsgespräch.**