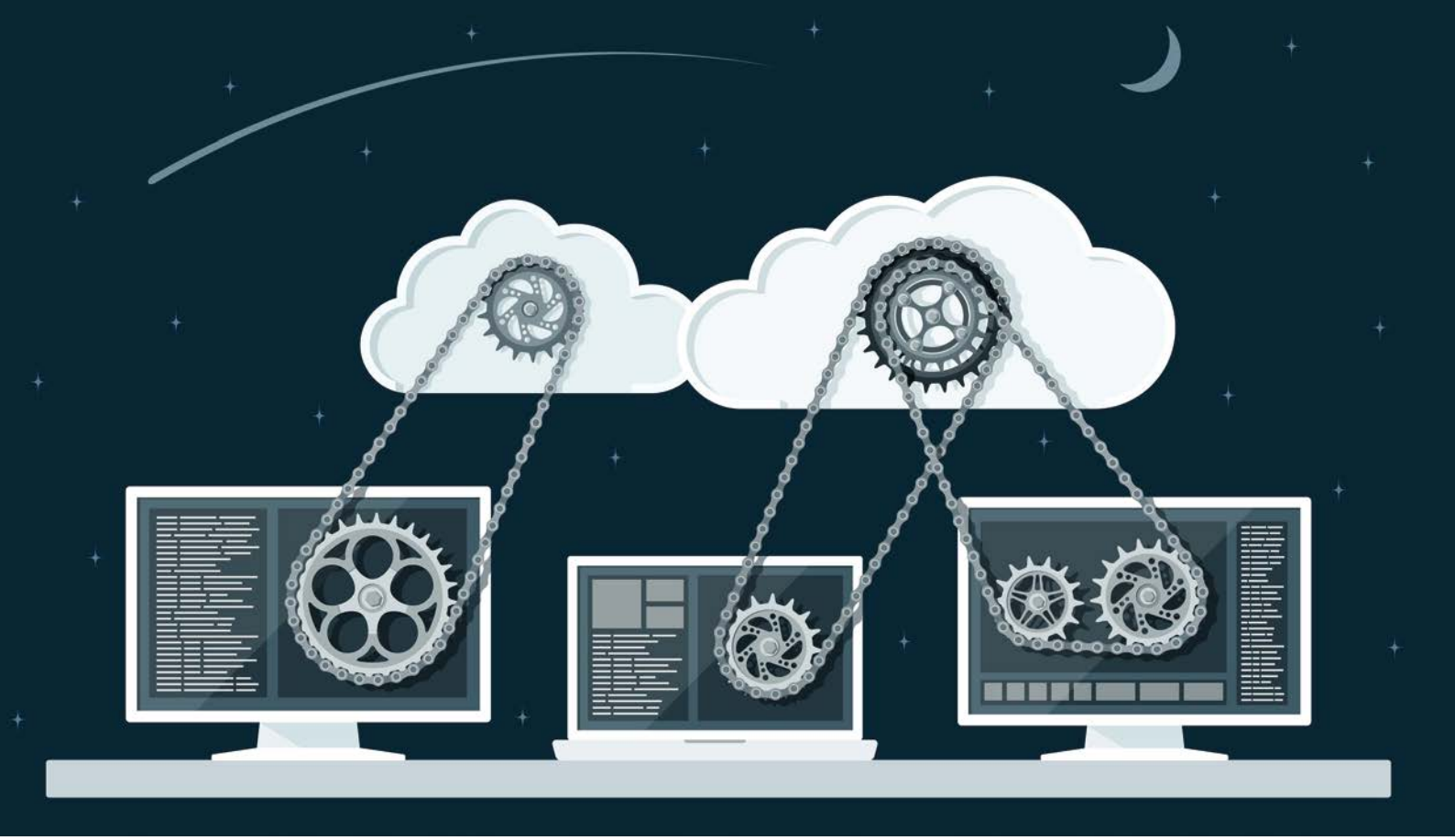

Cloud meets On-Premises – Herausforderungen in hybriden Infrastrukturen

Danilo Schmiedel, OPITZ CONSULTING Deutschland GmbH

In der heutigen digitalen Welt entsteht eine Vielzahl neuer IT-Lösungen, die Cloud-Dienste mit vorhandenen lokalen Systemen kombinieren. Die Folge sind hybride Architekturen, in denen die konsistente End-to-End-Verwaltung, Überwachung und Protokollierung über die gesamte Anwendungslandschaft hinweg besondere Herausforderungen mit sich bringen. Zusätzliche Anforderungen bestehen hinsichtlich Datenschutz, System-Integration und Kosten-Management. Der Artikel erläutert verschiedene Lösungsstrategien und Best Practices.

Die Lösungen zur Digitalisierung verändern auch die klassische Infrastruktur – alles wird Software. Wir sprechen heute von „Software-Defined Network" und „Software-Defined Infrastructure". Die meisten Unternehmen nutzen dafür Cloud-Lösungen mit unterschiedlichen Liefer- und Service-Modellen. In Cloud-Umgebungen ist für die Bereitstellung neuer virtueller Maschinen nur noch ein einfacher API-Aufruf nötig; diese Maschinen werden also nicht mehr von Hand eingerichtet, sondern automatisch durch sogenannte „Infrastructure-as-Code-Lösungen" (wie Oracle Cloud Stack Manager oder Terraform) provisioniert.

Die Evolution von Cloud und Software verstärkt sich gegenseitig. Anstatt auf diese Entwicklung mit Bestrebungen zur Zentralisierung und Standardisierung zu antworten, um somit in der Folge wieder die Geschwindigkeit zu hemmen, sollte die IT einen „Design for Change"-Ansatz verfolgen und diesen in eine reaktive Infrastruktur integrieren. Hybride Infrastrukturen vereinen die Stärken von On-Premises-Ansätzen mit der Flexibilität des Cloud Computing.

Cloud meets On-Premises

Die Vorteile und das Versprechen des Cloud Computing liegen auf der Hand: IT-Power aus der Steckdose. Die Kosten sind nun reine Verbrauchskosten und be-

ziehen sich auf die tatsächliche Nutzung, basierend auf nutzungsbezogenen Preismodellen. Betriebswirtschaftlich ist somit eine Wandlung der Kapitalbindung durch IT-Infrastruktur (CAPEX) in operative Betriebskosten (OPEX) möglich. Neben den betriebswirtschaftlichen Überlegungen hinsichtlich Investitionsschutz und Abschreibungszeiträumen bedingen im Endeffekt zwei Kriterien die Implementierungsentscheidung für oder gegen eine Cloud-Lösung: Datenschutz und Kosten.

Datenschutz und Datensicherheit

Zunächst ist es wichtig, die Begriffe „Datenschutz" und „Datensicherheit" voneinander abzugrenzen. Je nach Betrachtungsweise wird Datenschutz verstanden als Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch Schutz der Privatsphäre. Das Bundesdatenschutzgesetz (BDSG) regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die Auskunft zu sachlichen oder persönlichen Verhältnissen einer Person geben. Schutzziel ist die informationelle Selbstbestimmung; betroffene Personen haben also das Recht zu erfahren, wo und wie die Daten verarbeitet werden.

Die Datensicherheit bezieht sich auf den technischen Schutz von Daten jeglicher Art vor Verlust, Manipulationen und andere Bedrohungen. Hinreichende Datensicherheit ist eine Voraussetzung für effektiven Datenschutz. Als Schutzziele sind insbesondere Verfügbarkeit, Integrität und Vertraulichkeit zu nennen.

Für beide Aspekte ist es notwendig, die gewachsenen, oft schon veralteten Regelungen zu hinterfragen, um nicht ohne Not eine Entscheidung zu Ungunsten einer Cloud-Lösung zu treffen. Mit der neuen EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz 2018 (BDSG-2018), die ab 25. Mai 2018 in Kraft treten, gewinnt diese Frage an Bedeutung. Das gesamte System wird durch die neuen Regeln zwar weitestgehend nach deutschen Standards, aber grundlegend neu gestaltet. Aufgrund der umfassenden technischen und organisatorischen Maßnahmen der Anbieter kann der Weg in die Cloud sogar zu einer Verbesserung des eigenen Datenschutzes und der Datensicherheit beitragen. Schließlich verfügen unternehmenseigene Rechenzentren häufig nicht über die strengen Qualitätsstandards und aktuellen Zertifizierungen auf dem Niveau der Cloud-Anbieter *[1]*.

Nach §11 BDSG ist Cloud Computing eine Auftragsdatenverarbeitung (ADV). Es wird zwischen Nutzer (= Auftraggeber) und Auftragsdatenverarbeiter (= Auftragnehmer beziehungsweise Cloud-Anbieter) unterschieden. Der Nutzer ist dabei die verantwortliche Stelle und trägt die Sorgfaltspflicht für eine ordnungsgemäße Datenverarbeitung (DV). Er muss den Zweck der DV definieren und Weisungen erteilen. Der Auftragsdatenverarbeiter handelt ausschließlich auf Weisung des Cloud-Nutzers. Kundendaten werden nur im Umfang des gewählten Cloud Service verarbeitet. Konkret müssen in der ADV die folgenden Punkte geregelt sein:

- Zweck der Auftragsverarbeitung
- Weisungen des Auftraggebers
- Beschreibung und Überprüfung konkreter technologischer und organisatorischer Sicherheitsmaßnahmen
- Vereinbarung zur Löschung der Daten
- Regelung zu Subunternehmern
- Kontrollrechte des Cloud-Nutzers und Informationspflichten des Cloud-Anbieters
- Wahrung der Betroffenenrechte
- Rückgabe nach Vertragsbeendigung

Für die Nutzung von Cloud Services sind konkret technisch-organisatorische Sicherheitsmaßnahmen zu ergreifen, die es dem Anbieter ermöglichen, seine Sorgfaltspflichten zu wahren und die Kontrolle über die Datenverarbeitung zu behalten. Dazu müssen insbesondere die folgenden Datenschutzziele eingehalten werden:

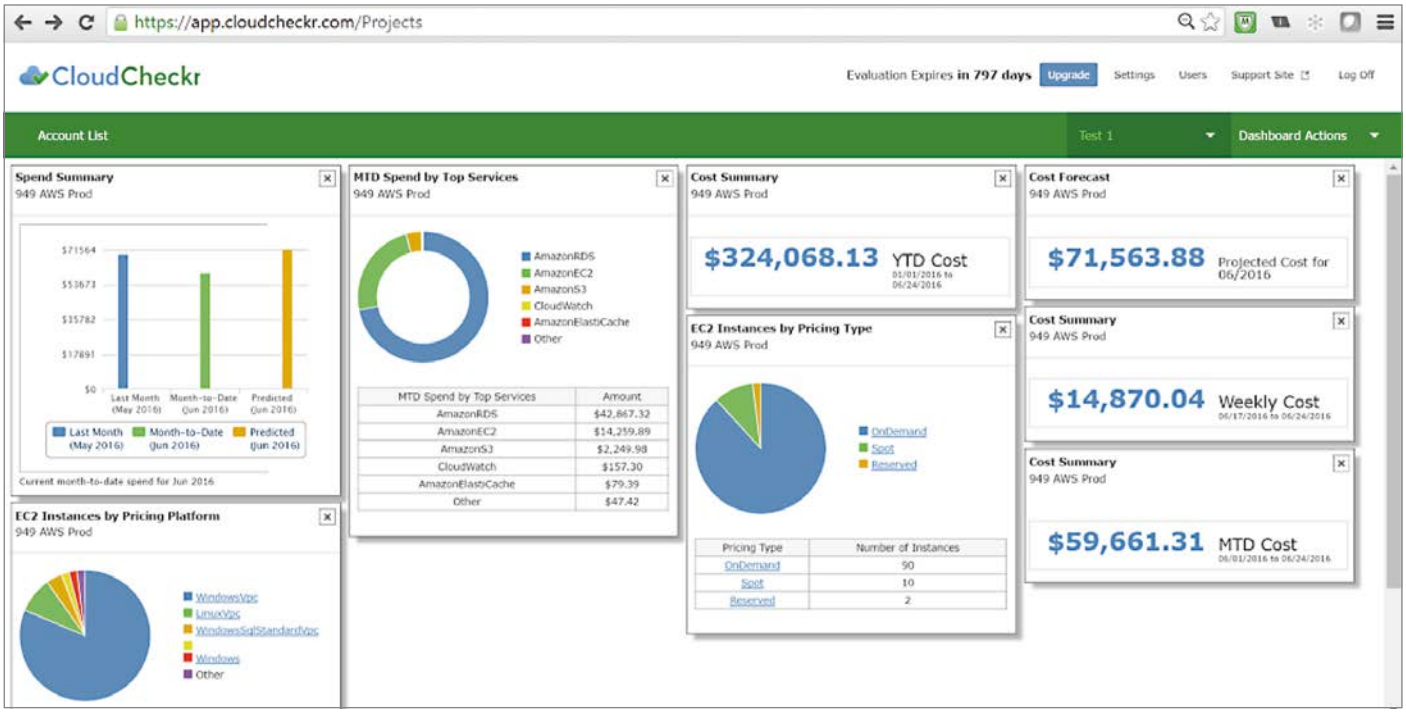

Abbildung 1: Multi-Cloud-Kosten-Management mit CloudCheckr

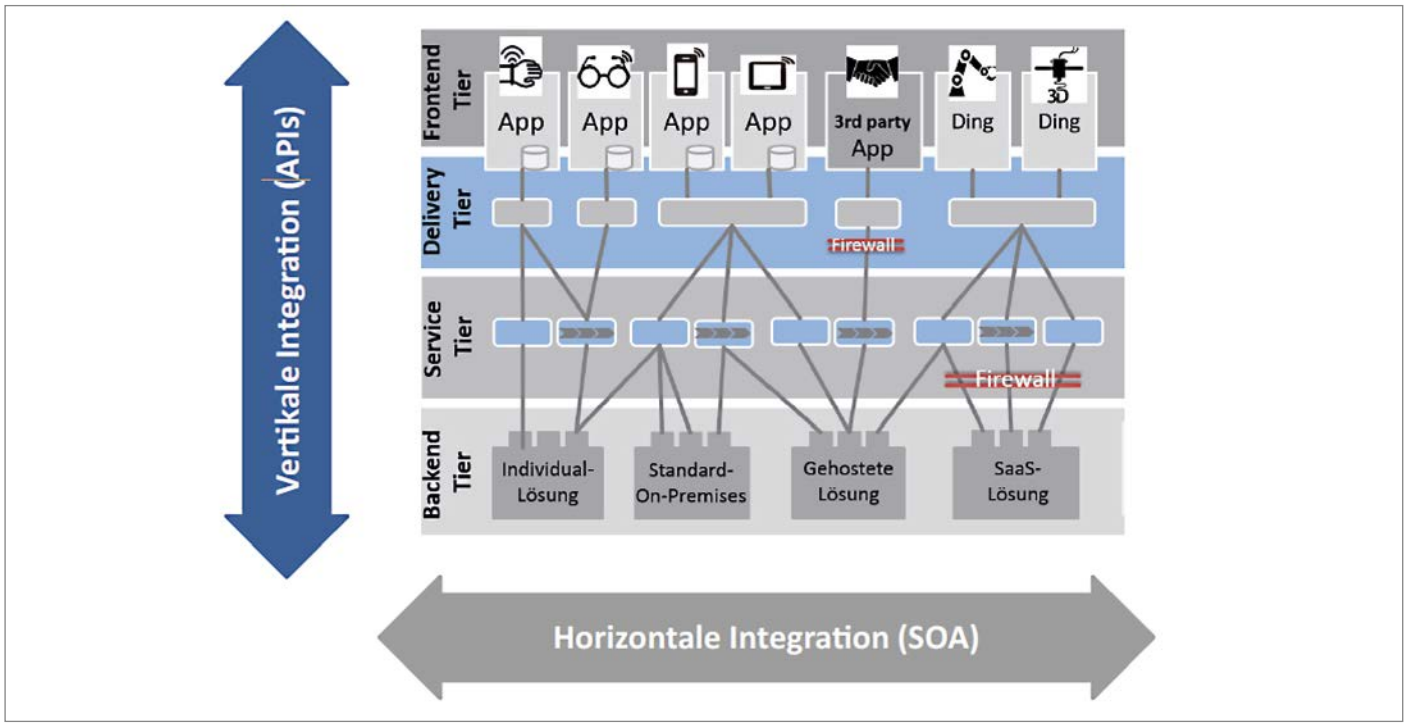

Abbildung 2: Horizontale und vertikale Integration

Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, geteilte Verarbeitung, Auftragskontrolle und Verfügbarkeitskontrolle.

Modell der geteilten Verantwortung

Wer nun glaubt, dass Daten in der Cloud zwangsläufig Kontrollverlust bedeuten, der irrt. Dieser Mythos hält sich hartnäckig. In Wahrheit ist es jedoch so, dass ein

Cloud-Nutzer die Kontrolle über die Daten behält und auch für diese

verantwortlich ist (Shared Responsibility Model). Oracle unterteilt die Verantwortlichkeiten von Anbieter und Nutzer in folgende Bereiche: Identity and Access Management (IAM), Workload Security, Data Classification and Compliance, Host Infrastructure Security, Network Security, Client and End-Point Protection sowie Physical Security *[2]*.

Zusammenfassend ist der Cloud-Anbieter verantwortlich für die Sicherheit der zugrunde liegenden Cloud-Infrastruktur. Diese besteht aus den Einrichtungen, der Hardware, der Software und dem Netzwerk. Demgegenüber ist der Cloud-Nutzer verantwortlich für die Sicherheit in der Cloud. Durch Verschlüsselung der Daten und Speicherung der Schlüssel „im eigenen Haus" hat der Cloud-Nutzer die alleinige Hoheit über die Daten. Er ist verantwortlich für Management und Überwachung des Zugriffs durch individuelle Benutzerkonten sowie der Aktivitäten in diesen Konten. Für die meisten Cloud Services ist das Risiko des Kontrollverlustes demnach vergleichbar mit dem Risiko bei herkömmlichen IT-Infrastruktur- oder IT-Outsourcing-Anbietern *[1]*. Zwingende Voraussetzung für den erfolgreichen Aufbau hybrider Cloud-Infrastrukturen ist die sorgfältige Betrachtung folgender Rahmenbedingungen:

- Klärung gesetzlicher Anforderungen
- Prüfen der vertraglichen Gegebenheiten zwischen Cloud-Anbieter und Nutzer
- Prüfung der technischen und organisatorischen Sicherheitsmaßnahmen des Cloud-Anbieters und Mapping zu Datenschutzzielen (unterteilt in Verantwortlichkeiten nach Cloud-Anbieter und Cloud-Nutzer)
- Ermittlung des Schutzbedarfs und Zuordnung zu den Schutzklassen
- Ermittlung der technisch-organisatorischen Sicherheitsmaßnahmen, die für die jeweiligen Schutzklassen zu ergreifen sind, beziehungsweise Klärung, ob Daten einer Schutzklasse überhaupt in der Cloud verarbeitet werden dürfen
- Risiko-Analyse

Kosten

Eine besondere Herausforderung in hybriden Infrastrukturen stellt das Kostenmanagement dar. „Pay as you go", „OPEX" statt „CAPEX", Orchestrierung von Services in Minuten, Abfangen von Lastspitzen, automatische Skalierung und Datensicherheit sind zwar Vorzüge, die eine Public Cloud zu bieten hat, aber nur wer sie richtig nutzt, spart Geld, ist schneller, flexibler und damit innovativer. In der Public Cloud ersetzen Services und Subscriptions die alten Lizenzmodelle. Man bezahlt in der Public Cloud also nur für das, was man nutzt. Nicht mehr und nicht weniger. Auch hier gibt es jedoch Unterschiede, über welche Metriken die Abrechnung erfolgt:

- Minutengenaue Abrechnung
- Vergünstigungen beim Erwerb von Jahrespauschalen
- Anrechnung eigener Lizenzen (BYOL)
- Ersteigern von Rechenkapazität für kurzfristige Nutzung
- Abhängige Preisgestaltung vieler Anbieter je nach Durchsatzrate, Art des Speichers und Datenverkehr

Die Liste ließe sich noch beliebig fortführen. Hier zeigt sich die Komplexität der Preisgestaltung in der Public Cloud. Kostentransparenz ist daher ein entscheidender Faktor:

Welche Services können welcher Kostenstelle zugeordnet werden? Wie stehen die geplanten Kosten zu den tatsächlich angefallenen Kosten im Verhältnis? Wie lässt es sich vermeiden, dass ungenutzte Cloud-Ressourcen unnötig Kosten verursachen? Welche Auswirkung haben Auto-Scaling und Serverless-Ansätze auf die Kostenentwicklung?

Die Implementierung hin zu mehr Kostenkontrolle erfolgt in zwei Schritten. Zunächst sollte die Organisation Rollen und Verantwortlichkeiten für zentrale IT- und Finanzteams sowie Cloud-Ressourcenbesitzer in den Geschäftsbereichen definieren. Daraufhin ist die Etablierung einer kollaborativen Kostenmanagement-Plattform zur effizienten und kontinuierlichen Kontrolle und Optimierung der Kosten zu empfehlen. Cloud-Anbieter wie Oracle bieten eigene webbasierte Kosten-Explorer für das Monitoring ihrer Services an. Allerdings handelt es sich hierbei zumeist nur um eine Sicht auf die aktuellen „IST"-Kosten. Mit Cloud-Checkr *[3]*, Cloudability *[4]* und RightScale *[5]* gibt es deutlich ausgereiftere Multi-Cloud-Kostenmanagement-Lösungen am Markt. Zu ihren Kernfunktionalitäten gehören Dashboards zur Kosten-Analyse, Showback- und Chargeback-Berichte, Trigger zum Auslösen von automatisierten Aktionen, Kollaborationsmöglichkeiten, Alerting und zentralisierte Optimierungsempfehlungen *(siehe Abbildung 1)*. Keine der genannten Lösungen bietet Stand heute eine Integration zur Oracle Cloud an. Zumindest bei *[3]* steht diese gemäß Herstellerangabe jedoch auf der Roadmap.

Interoperabilität und Integration

Der Trend von Cloud Computing und SaaS-Lösungen verschärft die Notwendigkeit hybrider Infrastruktur-Architekturen für die Applikationslandschaft. Dies erfordert eine modulare Architektur des Backends und die Entkopplung der Frontend-Komponenten. Die Release-Zyklen der einzelnen Komponenten dürfen nicht die Plattform als Ganzes kompromittieren. Hinsichtlich der Balance der On-Premises-Lösungen zu den Cloud-Lösungen spricht man vom „Center of Gravity", womit der Anteil der Cloud-Lösungen in Bezug zu den On-Premises-Installationen ausgedrückt wird. Je höher der Einsatz unterschiedlicher Cloud-Lösungen ist, desto eher verschiebt sich das „Center of Gravity" in die Cloud und somit auch die Integrations-Plattform, die näher an den Ursprung der Daten rückt *[6]*.

Durch die gewachsene Dezentralisierung der Applikationen besteht die Gefahr von Wildwuchs und potenzieller Unbeherrschbarkeit. Deshalb empfiehlt sich eine Einteilung in horizontale und vertikale Integrationsaspekte *(siehe Abbildung 2)*. Die horizontale Integration bezeichnet den klassischen System-zu-System-Ansatz. Ihm liegen oftmals schwergewichtige proprietäre Protokolle, technische Schnittstellen, Batch-basierter Datenaustausch und asynchrone Interaktionspatterns zugrunde. Klassischerweise kommen hierfür zentrale Integrationsplattformen (wie Oracle Integration Cloud Service) mit standardisierten Adaptern zum Einsatz.

Bei der Einführung von zentralen Integrationslösungen in hybriden Cloud-Infrastrukturen ist besonderes Augenmerk auf das Design der Gesamt-Architektur zu legen, da der Datentransfer ein entscheidender Kostentreiber sein kann. Durch ungünstig gewählte Kommunikationsstrecken können doppelte Kosten beim Datenaustausch zwischen Systemen entstehen – etwa, wenn die gleichen Daten mehrfach über verschiedene Regionen und unterschiedliche Clouds transportiert werden. Dieses Problem verschärft sich speziell in Multi-Cloud-Landschaften. Kontinuierliche Kostentransparenz und eine durchdachte Integrations-Architektur sind hier die wesentlichen Erfolgsfaktoren.

Die vertikale Integration ist eher nutzergetrieben und basiert auf leichtgewichtigen Protokollen und fachlich ausgerichteten Schnittstellen, die nahezu in Echtzeit antworten müssen. In den letzten Jahren hat hier das für hybride Infrastrukturen relevante „API Management" besonders an Bedeutung gewonnen *[7]*. Dabei steht die Bereitstellung von fachlich orientierten APIs im Fokus, die leicht verständlich und somit von einer breiten Masse nutzbar sein müssen. Dabei ist es sinnvoll, zwischen sogenannten „Single-" und „Multi-Pupose"-APIs zu unterscheiden – so wie im Projekt „Open Modern Enterprise Software Architecture" (OMESA) definiert *(siehe Abbildung 3)*.

OMESA wurde mit dem Ziel ins Leben gerufen, architektonische Best Practices in

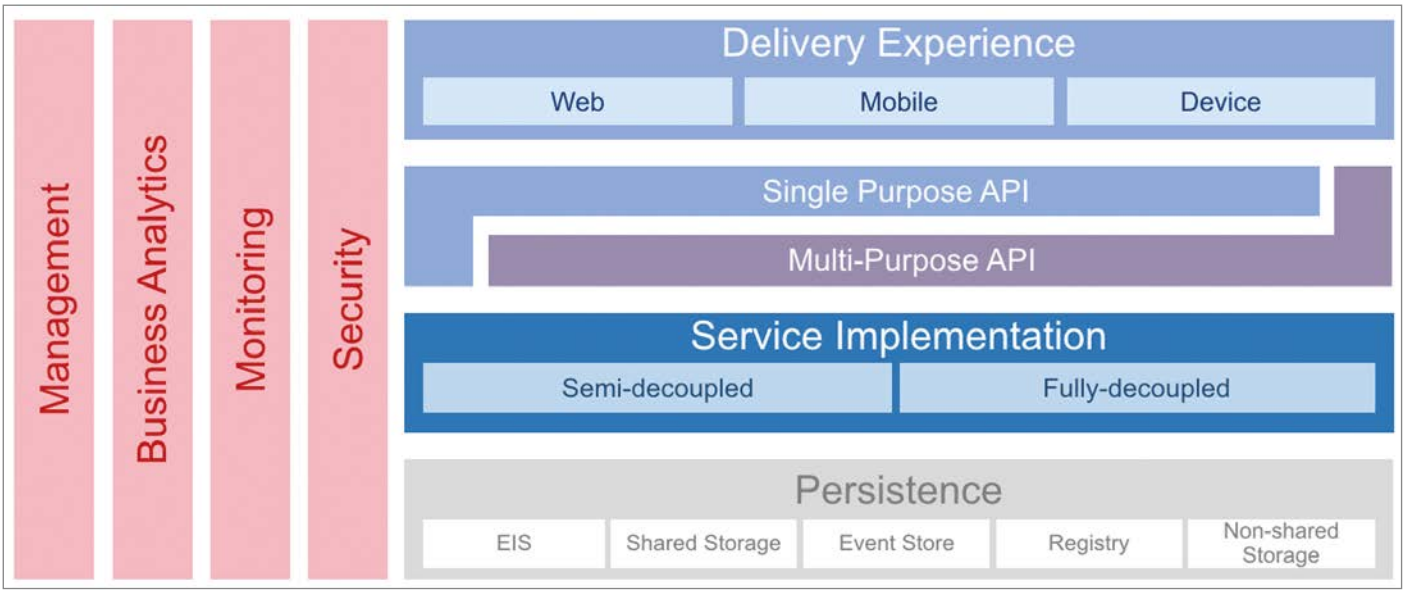

Abbildung 3: OMESA-Referenz-Architektur

moderne Architekturen zu integrieren und dabei zu berücksichtigen, dass neue und alte Komponenten koexistieren können. Es bietet Referenz-Architekturen und Leitprinzipien, die Architekten jeder Organisation dabei unterstützen, moderne Technologien und Architekturen aufzubauen und gleichzeitig die Schaffung von Mikrosilos oder Ad-hoc-Lösungen zu vermeiden. Das Projekt ist noch recht jung, bietet aber viele nützliche Ansätze zur Etablierung eines konsistenten API-Managements in hybriden IT-Infrastrukturen.

Bei der Erstellung von APIs ist es wichtig, einem API-First-Ansatz zu folgen. Dabei ist bereits im Vorfeld der App- beziehungsweise Backend-Entwicklung eine stabile API-Definition festzulegen, die den fachlichen Anforderungen gerecht wird. Abgestimmte und zentral erhältliche API-Style-Guides bilden dafür die Grundlage und definieren die Core-Prinzipien, Protokolle, Nachrichten-Formate, Datenmodelle, Typen, Testbarkeit, Wartung, Erweiterbarkeit, Skalierbarkeit, Ausführbarkeit und Benutzbarkeit. Für das konsistente Design gemäß API-First, kontinuierlichen Tests auf Basis integrierter API-Mock-Server, Versionierung und Kollaborationsmöglichkeiten bietet Oracle eine attraktive Lösung namens „Apiary" an *[8]*.

Nach Meinung des Autors ersetzen API-Management-Plattformen aber keinesfalls die klassischen Integrations-Plattformen – wenngleich die Feature-Sets entsprechender Produkte mitunter Überschneidungen aufweisen. Die wesentlichen Aufgaben der API-Plattformen lauten: Absicherung von Endpunkten, Auffindbarkeit, Verwaltbarkeit, Design-first und Monetarisierung. Integrations-Plattformen zielen auf Konnektivität, Transformation von Daten und Nachrichten-Formation sowie Caching und Skalierung ab. APIs sollten so schnell und schlank wie möglich sein. Sogenannte „API-Gateways" stehen häufig in einer Demilitarized Zone (DMZ). Sie validieren Anfragen und wehren sie gegebenenfalls ab. Sensible Daten dürfen nicht auf der Festplatte oder im Speicher der DMZ gespeichert sein.

Dies wird mithilfe der Integrations-Plattform gelöst. Deren Hauptaufgabe liegt in der Transformation komplexer Payloads und der Orchestrierung von Service-Aufrufen. Durch die Verwendung eines robusten Caching-Systems können Skalierbarkeit und hohe Leistung erreicht werden, während die Daten in einer ordnungsgemäß gesicherten Zone gehalten werden. Darüber hinaus stellt die Integrationsplattform die Konnektivität zu inkompatiblen Backend-Systemen (etwa als On-Premises) bereit. Die Verwendung von Adaptern in einem API-Gateway würde zu gesteigerter Komplexität auf dem API-Layer führen. Bedeutet dies aber, dass ein API-Gateway diese Funktionen niemals anbieten sollte? Nicht unbedingt. Es gibt Fälle, in denen es sinnvoll ist, Daten in einem API-Gateway zwischenzuspeichern oder sogar einfache Transformationen durchzuführen. Hier ist es schwer, ein „one size fits all" zu finden. Die Auswirkungen und Risiken sind demnach von Fall zu Fall zu entscheiden.

Betrieb in hybriden Infrastrukturen

Dieser Artikel behandelt insbesondere die Herausforderungen im Bereich des Datenschutzes, der Kosten und der System-Integration. Der Betrieb von hybriden Infrastrukturen verfügt über zusätzliche umfassende Anforderungen; dazu zählen insbesondere ein End-to-End-Infrastruktur- und ein Applikations-Monitoring, das sowohl Multi-Cloud als auch On-Premises-Systeme berücksichtigt. Weitere wichtige Aspekte sind umfassende Log-Auswertungen, Alerting, Aufgaben-Automatisierung sowie die proaktive Überwachung von Sicherheitsbedrohungen.

Die Oracle Management Cloud adressiert die meisten dieser Anforderungen *[9]*. Dabei handelt es sich um eine Suite integrierter Überwachungs-, Verwaltungs- und Analyse-Cloud-Angebote. Die Lösung wurde speziell für hybride Umgebungen entwickelt: On-Premises, Oracle Cloud und Cloud-Services von Drittanbietern. Betriebsdaten in IT-Organisationen, einschließlich maschinengenerierter Daten, können unterschiedlicher Art und Größe sein und werden häufig in mehreren Systemen gespeichert. Mit der Oracle Management Cloud lassen sich hochgeladene Daten in einer einzigen einheitlichen Plattform speichern und auswerten. Die Plattform analysiert Daten automatisch auf Basis von Machine-Learning-Algorithmen und Korrelation. Die Daten der zu überwachenden Entitäten (wie Datenbanken, Host Server, Compute-Ressourcen und Applikationsserver) werden von Agenten gesammelt. Zur Vertiefung empfiehlt sich einen Blick in das umfassende Dokumentationsangebot *[10]*.

Fazit

Hybride Architekturen erhöhen häufig die Komplexität, sind allerdings essenziell, um im Zeitalter der Digitalisierung Schritt halten zu können. Dafür ist es wichtig, dass das Modell der geteilten Verantwortung verinnerlicht wird. Integrations-Plattformen stellen die Konnektivität sicher und ermöglichen die Zusammenführung neuer Services mit vorhandenen Systemen (horizontale Integration). Für die Absicherung, Zugriffsbeschränkung und Monetarisierung von nutzerzentrischen APIs bietet sich die Etablierung einer API-Management-Plattform an. Nur wer in hybriden Infrastrukturen die volle Kostentransparenz besitzt, spart Geld und fördert Innovation.

Quellen

[1] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2012 zum Cloud Computing; Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Cloud Computing, 01.07.2012, *https://www.lda.bayern.de/media/wp196_de.pdf*

[2] Oracle Corporation: Oracle Cloud Infrastructure Security, *https://docs.us-phoenix-1.oraclecloud.com/Content/Resources/Assets/oci_security.pdf*

[3] *https://cloudcheckr.com*

[4] *https://www.cloudability.com*

[5] *https://www.rightscale.com*

[6] Jim Harris, The Cloud is shifting our Center of Gravity, 19. Juli 2012: *http://www.ocdqblog.com/home/the-cloud-is-shifting-our-center-of-gravity.html*

[7] *https://cloud.oracle.com/api-platform*

[8] *https://apiary.io*

[9] *https://cloud.oracle.com/management*

[10] *https://docs.oracle.com/en/cloud/paas/management-cloud/index.html*

Danilo Schmiedel
danilo.schmiedel@opitz-consulting.com