Whitepaper Multi-Cloud

Workstream	Cloud III – Cloud Integration in the Multiverse
Klassifikation	Öffentlich
Autoren	Wolfgang Wortmann Stefan Gerberding Thorsten Marhun Björn Oestrich Merve Yildiz
Versionsdatum	11.02.2020
Copyright	

1. Inhaltsverzeichnis

2. Einleitung

Cloud Computing ist heute ein Commodity Service der IT geworden. Der Einsatz von Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS)-Angeboten innerhalb der Unternehmens-IT ist heute Alltag.

Unter dem Begriff Cloud Computing hat sich ein neues Bereitstellungsmodell für IT-Dienstleistungen etabliert, IT-Dienstleistungen können von einem oder mehreren Cloud Service Providern bedarfsgerecht über das Internet bezogen werden. Die Cloud-Dienstleister erfassen den Ressourcenverbrauch und stellen den Nutzern lediglich die tatsächlich verbrauchten Ressourcen in Rechnung. Als Cloud Service Provider (CSP) werden in diesem Whitepaper alle Anbieter für Dienste im Bereich Infrastruktur (Infrastructure as a Service, IaaS, z. B. virtuelle Rechner und Netzwerke), Plattformen (Platform as a Service, PaaS, z. B. eine Datenbankplattform), Softwarelösungen (Software as a Service, SaaS, z. B. eine CRM-Lösung) oder Anwendungsservices (z. B. ein Bilderkennungsservice) bezeichnet. Die Zusammenfassung dieser Angebote wird in diesem Whitepaper als Cloud-Dienste bezeichnet.

Längst geht es nicht mehr darum, ob Cloud Services im Rahmen der IT-Strategie sinnvoll sind, sondern wie sich daraus der größte Nutzen ziehen lässt. Allerdings bringt der Einsatz von Cloud Service Providern auch Herausforderungen für die Unternehmen, dazu zählen zum Beispiel die komplexe Integration von Cloud-Diensten in die Unternehmens-IT oder das als „Vendor Lock-in“ bezeichnete Abhängigkeitsverhältnis zum Cloud Service Provider. Außerdem vergrößert sich nicht nur das Service-Portfolio der Cloud-Giganten ständig, hinzu kommen neue Technologien etwa aus der Open Source Community und jede Menge zusätzliche Fachbegriffe, die Entscheider kennen und einordnen können sollten. Somit steigt zunehmend auch die Komplexität.

Ein Multi-Cloud-Ansatz beginnt mit einer klassischen Make-, Take- (Nachbau einer Cloud mit verfügbaren Komponenten) oder einer Buy-Betrachtung für universelle CSP. Die Make- und Take-Betrachtungen liegen dabei eng beieinander und werden zumeist von internen Teilen der IT als Variante angeführt. Die Teilnehmer des Workshops haben allerdings festgestellt, dass die benötigten Ressourcen – Budgets, Skills, Infrastruktur – für diese Betrachtung nicht getragen werden können. Die Aufwände, um die generischen Basisservices eines CSP nachzubauen stehen bei keinem teilnehmenden Unternehmen im Verhältnis zum Nutzen daraus – auch im Besonderen mit Blick auf die IT-Security und Datenschutz als meist angeführte Argumente.

Eine Buy-Betrachtung eines universellen CSP ermöglicht dabei den direkten Ressourceneinsatz von Cloud-Diensten und damit eine Umsetzung der Cloud Services für die eigene Innovation. Somit ist die

Auswahl eines oder mehrerer CSP hauptsächlich auf deren Cloud Service Offering notwendig, um eigene Service-Bedarfe möglichst gut abdecken zu können.

Fünf Mitglieder des CBA Lab haben sich zusammengetan, um die Erfahrungen für eine Unternehmensarchitektur mit Cloud zusammenzutragen und daraus Best Practices für alle Mitglieder zu erarbeiten. Der Einsatz von einem Cloud Service Provider ist bei allen Mitgliedsunternehmen gegeben.

In diesem Sinne wurden vier Workshops veranstaltet, um den intensiven Erfahrungsaustausch unter den Mitgliedern zu ermöglichen und Input für das vorliegende Whitepaper zu sammeln. Dieses Whitepaper ist das Ergebnis der Workshops und der darauffolgenden zahlreichen Redaktionskonferenzen.

Das Whitepaper trägt die Erfahrungen der Mitglieder zu folgenden Themen zusammen:

- Entscheidungshilfe Provider Lock-in (Value vs. Control) & Multi-Cloud-Ansätze,
- Leitfaden für ein „angemessenes Architekturmanagement“ in der Cloud,
- Best Practices Integration der private und public Cloud mit On-Premise-Netzen und -Systemen.

3. Entscheidungshilfe Provider Lock-in: Value vs. Control & Multi-Cloud-Ansätze

Die Cloud-Dienste der CSP sind nicht standardisiert, auch wenn sich die Angebote der großen Anbieter sehr ähneln. Im Bereich IaaS und PaaS setzen viele CSP auf vergleichbare Software Stacks, die oft aus Open-Source-Angeboten übernommen und um Mehrwertdienste angereichert sind. Die angebotenen Infrastrukturen und Plattformen sind daher zwischen den CSP teilweise austauschbar.

Zu einem gewissen Grad kann ein Vendor Lock-in auf den CSP vermieden werden, falls nur Infrastruktur-Dienste oder eine Container-Ablaufumgebung benötigt werden. Beispielsweise bieten die meisten CSP eine Auswahl virtueller Server verschiedener Leistungsklassen mit Betriebssystemen aus den weit verbreiteten Linux-Distributionen oder verteilte Container-Ablaufumgebungen z. B. auf Basis Kubernetes[1] an. Darauf können Anwendungen ohne Vendor Lock-in betrieben werden (falls proprietäre Deployment-Automatisierung vermieden wird).

Die Entscheidung für die Angebote eines oder mehrerer CSP muss einer Cloud-Strategie folgen. Diese legt die Ziele und Rahmenbedingungen für den Einsatz von Cloud-Diensten für ein Unternehmen fest. Falls die Strategie den Einsatz von Cloud-Diensten z. B. nur für virtuelle Server vorsieht, kann ein Vendor Lock-in, wie oben skizziert, vermieden werden.

Typische Ziele einer Cloud-Strategie sind

- Umwandlung von Investitionen (in IT Hardware, CapEx) in Betriebskosten (Pay-Per-Use, OpEx),
- Verkürzung von Innovationszyklen und Erhöhung der Innovationsgeschwindigkeit,
- Unterstützung des Kerngeschäfts,
- Ermöglichung neuer Geschäftsmodelle,
- Schaffung von regional verteilten IT-Ressourcen zur Unterstützung weltweiter Geschäftsfunktionen,
- Erhöhung der Verfügbarkeit durch (geo-) redundante IT-Ressourcen.

Sobald die Strategie auch die Verwendung innovativer Dienste oberhalb der Infrastruktur vorsieht, ist ein Vermeiden eines Lock-in nicht mehr realistisch: Hierzu müsste die Anwendung so gestaltet werden, dass für jeden konsumierten Service alternative Dienste mindestens eines weiteren CSP verwendet werden können. Dazu müssten entsprechende Variationspunkte in der Anwendung vorgesehen werden oder eine Abstraktionsschicht (Broker) vor den CSP etabliert werden.

[1] https://kubernetes.io

Ein (technischer) Broker für mehrere CSP besteht einerseits aus Endpunkten für Anbieter abstrahierter Cloud-Dienste, hinter denen die entsprechenden konkreten Cloud-Dienste der unterschiedlichen CSP verfügbar sind. Andererseits realisiert er ein Regelwerk zur Auswahl des konkreten Cloud-Dienstes bzw. des CSP hinter dem abstrakten Cloud-Dienst.

Die Weiterentwicklung (die großen CSP bieten ständig neue innovative Dienste an) und der Betrieb dieses Brokers ist mit Zusatzaufwand verbunden und nach Auffassung der CBA-Lab-Mitgliedsunternehmen selten wirtschaftlich sinnvoll. Zudem können neue Dienste der CSP erst genutzt werden, wenn ausreichend viele CSP-Varianten diese Dienste anbieten und der Broker diese kennt und einsetzen kann. D. h. Innovation wird verzögert. Den Broker als nicht-technische Komponente in Form eines Kriterienkatalogs für die Auswahl der Cloud-Dienste der einzelnen CSP zu verwenden ist eine gute Alternative zum technischen Broker.

Kriterien, die für die Entscheidung für ein (nicht unbedingt technisches) Brokering sprechen, sind

- die Möglichkeit der Einrichtung eines Policy Enforcement Point für die Auswahl der geografischen Position, an dem ein Cloud-Dienst erbracht wird (Lage eines Rechenzentrums des CSP),
- Trennung von Mandanten,
- Einschränkung des genutzten Service-Portfolios der Anbieter,
- Überwachung von Compliance- und Datenschutzanforderungen,
- Überwachung von Governance-Vorgaben zur (Netz-) Sicherheit,
- Überwachung von Verfügbarkeitsanforderungen,
- Kostenkontrolle und Steuerung.

Aus denselben Gründen, die gegen einen technischen Broker sprechen, ist es daher auch selten wirtschaftlich, Anwendungen abhängig von den Tagespreisen der CSP für Cloud-Dienste automatisch auf den günstigeren Anbieter zu verschieben.

Dennoch ist eine Multi-Cloud-Strategie oft für die Umsetzung der Cloud-Strategie des Unternehmens sinnvoll. Multi-Cloud bedeutet die Verwendung von Cloud-Diensten ausgewählter, unterschiedlicher CSP, sodass Anwendungen nicht notwendigerweise Ablaufumgebungen auf allen ausgewählten CSP finden müssen. Es geht nicht darum, Anwendungen leicht verschieben zu können, sondern um die Möglichkeit, die Cloud-Dienste mit dem meisten Mehrwert für das Unternehmen aus dem Angebot ausgewählter CSP selektieren zu können. Dabei kann eine Anwendung nur Dienste eines CSP konsumieren oder Dienste unterschiedlicher CSP kombinieren. Der Vorteil des Multi-Cloud (Best of Breed) -Ansatzes ist die Verwendung der Innovationskraft der CSP bei gleichzeitiger Streuung des Risikos. Allerdings sollte die

Entscheidung für einen Einsatz von mehreren CSP auch bei Innovationsdruck und Service-Verfügbarkeiten niemals aus einem Projekt heraus getroffen werden. Projektbezogene Entscheidungen führen dazu, dass keine ordentliche Einbindung des CSP in die notwendigen Cloud-Management-Prozesse erfolgt und damit ein unkontrollierter Teil der Unternehmens-IT geschaffen wird.

Für Unternehmen mit wachsendem Personalbedarf für innovative Themen bietet der Multi-Cloud-Ansatz gleichzeitig eine Chance, Know-how-Träger unterschiedlicher technischer Herkunft, d. h. mit technischer Expertise unterschiedlicher CSP einzustellen.

Dieser Vorteil kann für andere Unternehmen mit anderen Rahmenbedingungen ein Nachteil des Multi-Cloud-Ansatzes sein: Für die Multi-Cloud wird mehr unterschiedliches Know-how benötigt und die Integrationskomplexität steigt, bspw. sind komplexere Netzwerklösungen zur Einbindung der verschiedenen CSP notwendig.

Aktuelle Informationen zur Auswahl von CSP und einen Vergleich liefern viele Analysten[2]. Die folgenden Aspekte sind den Mitgliedsunternehmen im CBA Lab für die Entscheidung für einen Multi-Cloud-Ansatz wichtig. Die Relevanz dieser Aspekte und deren Gewichtung ist von der spezifischen Cloud-Strategie des Unternehmens abhängig.

- Risikostreuung, in Bezug auf
  - Vendor Lock-in (bspw. durch Migrationsmöglichkeiten),
  - Verfügbarkeitseinschränkungen,
  - Compliance Einschränkungen (z. B. wegen des Gerichtsorts des CSP),
- Reaktionsfähigkeit in Bezug auf Kosten (nicht als strategischer Treiber),
- Integrationsfähigkeit, Integrationskomplexität und Interoperabilität der Cloud-Dienste in die eigene Unternehmens-IT,
- Quality of Service der CSP in Bezug auf
  - Verfügbarkeit,
  - Security,
  - Compliance,
- Support-Fähigkeit durch den CSP bzgl.
  - Automatisierung und
  - Unterstützung bei der Anbindung der Cloud an das Unternehmens-Netzwerk,
  - Migration von Anwendungen in die Cloud und

[2] Neben den großen Analysten wie Gartner und Forrester gibt es zahllose (meist weniger detailliert recherchierte) Vergleiche von CSP und Kriteriensammlungen im Internet. Ein Beispiel hierfür ist http://comparecloud.in/

    - Anwendung und Integration von Cloud-Diensten,
    - Verfügbarkeit von Cloud-Diensten in relevanten geografischen Regionen,
- Support-Fähigkeit der eigenen Organisation im Unternehmen für bestimmte Technologien und Architekturen mit Relevanz für die Auswahl von CSP,
- Feature-Portfolio, z. B.
    - Innovative Cloud-Dienste (bspw. für Künstliche Intelligenz, Internet of Things, Advanced Analytics),
    - Transformationsunterstützung (bspw. für Migrationsdienste für Server und Datenbanken, Massendatentransfer),
    - Security (bspw. Key Management, Auditierbarkeitsunterstützung, Angriffsabwehr),
- Erweiterte Recruiting-Möglichkeiten durch das breitere Angebot bei Nutzung unterschiedlicher CSP,
- Verfügbarkeit von Skills und einem Ökosystem für den CSP am Markt,
- Reifegrad des CSP.

Die Mitgliedsunternehmen des CBA Lab teilen die Einschätzung, dass die Partnerschaft mit zwei größeren CSP im Allgemeinen ausreichend ist, um die Cloud-Strategie umzusetzen.

Migrationsszenarien bei einem Anbieterwechsel sind klassische Transformationsprojekte und bedürfen einer zentralen Steuerung. Da die Multi-Cloud-Fähigkeit einzelner Anwendungen üblicherweise nicht wirtschaftlich ist, wie bereits dargestellt wurde, müssen die Anwendungen und ihre Deployment-Automatisierung einzeln auf den oder die neuen (oder verbleibenden) CSP migriert werden. Dabei ist die Migration zwischen verschiedenen IaaS oder von containerisierten Anwendungen naturgemäß leichter als die von Anwendungen, die proprietäre Anwendungsservices verschiedener CSP konsumieren. Oft gibt es ähnliche Cloud-Dienste, die aber nicht kompatibel sind (bspw. für Serverless Computing), bei denen die Cloud-Dienste iterativ von einem CSP auf einen anderen reimplementiert werden müssen.

Um die Komplexität einer Multi-Cloud-Strategie zu beherrschen und die Herausforderungen zu meistern, ist es notwendig, das Enterprise-Architektur-Management (EAM) auf die o. g. Themen zu fokussieren. EAM muss sich dabei auf den Geschäftsnutzen und die Unterstützung des Geschäfts des eigenen Unternehmens durch Cloud-Dienste konzentrieren und nicht auf der technologischen Ebene verbleiben. Entscheidungen müssen regelmäßig in Bezug auf die Cloud-Strategie überprüft werden. Im Gegensatz zu einem Outsourcing muss auf jeden Fall IT-Know-how im Unternehmen verbleiben: Dies wird mindestens für die Steuerung der CSP, die Integration und das EAM benötigt, selbst wenn keine eigene Anwendungsentwicklung existiert.

Das Know-how, welches im Unternehmen für die Nutzung und Umsetzung von Cloud-Diensten benötigt wird, steigt mit der Komplexität der aus den Cloud-Diensten der CSP realisierten Lösungen. Falls nur IaaS-Dienste konsumiert werden, ist geringeres Know-how notwendig als bei der Verwendung von PaaS oder dem gesamten Portfolio eines CSP.

Der Einsatz von SaaS hat einige spezielle Aspekte für die Unternehmens-IT. Unter SaaS wird der Einsatz einer Lösung für eine Geschäftsfunktion verstanden, der über den Einsatz einzelner Anwendungsservices als IT-Unterstützung für Teile von Geschäftsfunktionen hinausgeht, wobei diese Lösung als Cloud-Dienst erbracht wird (bspw. ein CRM-System oder ein ERP-System). Der Anbieter einer SaaS ist damit ein Software-Anbieter und ein CSP (mit möglicherweise nur einem Cloud-Dienst im Portfolio).

Viele seit Langem am Markt befindliche Anbieter von SaaS haben ihre Anwendungen noch nicht für die Herausforderungen der Cloud-Integration und der Digitalisierung angepasst. Diese Anwendungen sind noch auf die früheren Outsourcing-Geschäfte ausgerichtet und haben monolithische Architekturen, sodass sich einzelne Geschäftsfunktionen der Lösung oft nicht über APIs als Services ansprechen lassen und eine kleinteilige Integration in die Unternehmens-IT nicht möglich ist. Offene Wertschöpfungsketten können so nicht erstellt werden, bei denen die IT-Unterstützung für die Wertschöpfungskette nicht Ende-zu-Ende unter der Kontrolle eines einzelnen Unternehmens ist, sondern aus Teillösungen oder Teilprozessen einer Gemeinschaft von Geschäftspartnern zusammengesetzt wird.

Bei der Auswahl von SaaS ist daher darauf zu achten, dass die Geschäftsfunktionen, Daten und ggf. das User Interface der Lösung sich in die Prozesse des eigenen Unternehmens und seiner Partner integrieren lassen. Alle Kriterien bei der Auswahl von CSP gelten zusätzlich auch hier. Das Risiko des Vendor Lock-in bei SaaS wird im Allgemeinen höher angesehen als bei CSP.

Viele Anbieter von SaaS adaptieren ihre Anwendungsarchitektur und ihr Service-Portfolio an die Anforderungen offener, interoperabler Services. Insbesondere ergänzen SaaS-Anbieter ihre Lösungen um allgemeinere Cloud-Dienste, welche die Möglichkeit bieten, die SaaS über Variationspunkte anzupassen, zu erweitern und Zusatzlösungen bereitzustellen. Eine Konvergenz der SaaS-Anbieter mit CSP kann beobachtet werden.

4. Leitfaden für ein „angemessenes Architekturmanagement“ in der Cloud

Die Einführung von Cloud-Diensten macht das Enterprise-Architektur-Management (EAM) nicht obsolet, jedoch ändert sich die Arbeitsweise, das EAM muss vor allem flexibler werden. Die eigentliche Kernaufgabe bleibt bestehen: die transparente Umsetzung der Geschäfts- und IT-Strategie zur Architektur. Neue Themen wie agiles Projektmanagement oder eine effiziente enge Zusammenarbeit von Entwicklung, Betrieb und Qualitätssicherung (DevOps) erfordern Anpassungen von Organisation, Prozessen, Implementierung und Fähigkeiten der Mitarbeiter. Die Weiterbildung der Mitarbeiter im EAM spielt dabei eine zentrale Rolle.

Die Arbeit im EAM kann dadurch viel konkreter werden, sodass bei agilen Projekten Architekturentscheidungen in kürzeren Zyklen (z. B. Sprints) in Zusammenarbeit mit einem DevOps-Team kleinteiliger getroffen werden und nicht auf der Ebene von Projekten. In großen Organisationen stellt sich allerdings die Frage, ob eine Beteiligung des EAM in Sprints skaliert.

Begleitet werden Cloud-Einführungen oft von einem Paradigmenwechsel: statt langfristig festgelegter Zielarchitekturen werden diese bei iterativen Ansätzen zur Erreichung von Zielen während des Prozesses durch wachsende Erfahrungen angepasst.

Klassische Projektorganisationen und Hierarchiestrukturen stoßen dabei an ihre Grenzen und erfordern eine Neuorganisation.

Erfolgreiches EAM entwickelt sich weiter von einer zentralen Planung und Governance-Abteilung hin zu einem flexiblen Supporter und Enabler der Fachbereiche und Unternehmens-IT. EAM betrachtet dabei alle Architekturebenen mit Tipps/Best Practices/Guidelines/Hilfestellungen und Vorgaben.

Doch was ändert sich für EAM durch die Einführung von Cloud-Diensten zusätzlich zu On-Premise?

- Governance
  - Um die Komplexität einer Multi-Cloud managen zu können wird empfohlen, ein entsprechendes Cloud-Management-Framework aufzusetzen.
- Perimeterschutz
  - Anwendungen befinden sich nicht notwendigerweise in einem gemeinsam geschützten Netzwerkbereich, d. h. es müssen Security-Anforderungen anders umgesetzt werden.
- Technologieportfolio

  - Cloud-Lösungen bringen eine Vielzahl neuer Technologien und Services mit sich. Dies erfordert eine intensivere Bewertung und die Bündelung von spezifischem Know-how in Technologiepools. Fachbereiche vertiefen sich zunehmend in IT-Themen, daher ist die Bildung und Unterstützung von Communities zum Wissensaustausch notwendig. Die Benennung von Ansprechpartnern für bestimmte Cloud-Technologien bzw. Technologieportfolios erleichtert den Austausch ('Touchpoints'). Gilden von Software- und Infrastrukturarchitekten aus dem operativen Umfeld helfen, Leitplanken für die Nutzung von Technologien zu setzen.
- Kostensteuerung
  - Die Steuerung von Kosten geht mehr in Richtung der tatsächlich genutzten Dienste (Pay-Per-Use) als über starre Servicevereinbarungen. Die jahresbezogene Kostenplanung muss auf den neuen Dienst angepasst werden.
  - Ein Schwenk auf ein aktives Kostenmanagement auf Serviceebene löst die jahresbezogene Kostenplanung ab: Das Cloud-Management meldet sich mit Optimierungsvorschlägen bei den Servicenutzern/Entwicklungsteams und Betriebsteams und hilft so, Kosten zu steuern.
- Security
  - Data Security und Data Compliance gewinnen große Bedeutung, da die Daten nicht mehr über einen eigenen Rechenzentrumsbetrieb abgesichert werden. Entscheidende Frage ist oft, wo sich die Daten physikalisch in der Cloud befinden und wie der Zugriff darauf abgesichert ist.
  - Data Continuity muss ebenfalls kritisch hinterfragt werden. In einem eigenen Rechenzentrumsbetrieb wurden dazu Services wie Backup und Disaster Recovery zentral zur Verfügung gestellt. In der Cloud sind diese Services nicht immer zentral organisiert, sondern werden von einzelnen Projekten in ihrer eigenen Umgebung verantwortet, im Wesentlichen durch die Entwickler, wodurch deren Verantwortung steigt. Während im eigenen Rechenzentrumsbetrieb zum Beispiel eher der Fokus auf Perimeterschutz rund um das Rechenzentrum liegt, rücken im Cloud-Umfeld eher Bedrohungen durch Hackerangriffe in den Mittelpunkt, deren Häufigkeit ständig ansteigt.
- Know-how
  - Neue EAM-Konzepte entstehen und müssen an die Entwickler-Community, die Fachbereiche und den Betrieb vermittelt werden.

    - Die von CSP angebotenen Dienste und Lösungsarchitekturen müssen gelernt werden und von der EAM-Organisation definierte Regelwerke müssen bekannt sein.
    - Eine Art „Führerschein“ kann helfen, diese Kenntnisse zu erwerben und zu überprüfen.
    - Das Wissen um Cloud-Services und deren Ausprägung muss eher breit als tief sein.
- Toolchain
    - Die Continous Integration / Continous Delivery (CI/CD) Toolchain sollte durch DevOps-Teams definiert und publiziert werden.
    - Durch eine definierte Toolchain können Governance-Anforderungen besser definiert werden, wie zum Beispiel Built-in Security und Compliance.

EAM kann helfen, die Rolle der Unternehmens-IT in den Cloud-Services zu definieren, um ein entsprechendes zentrales Service-Portfolio für das Business proaktiv anbieten zu können, ohne komplett demand-getrieben zu sein. Dazu gehören z. B.

- die Steuerung des CSP,
- die Vorfinanzierung durch die Unternehmens-IT bzw. ein CIO-Budget und
- das Angebot zentral betriebener IT-Services.

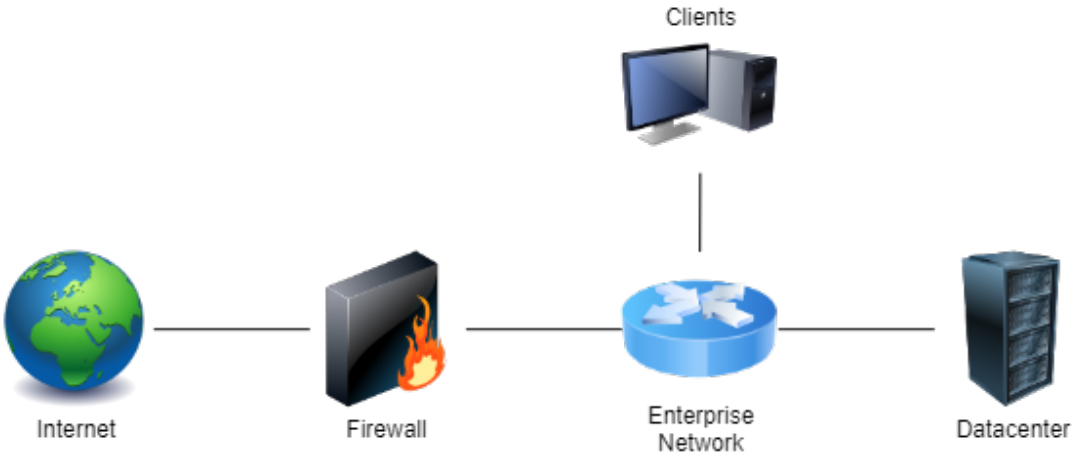
Die veränderten Anforderungen an die IT müssen neu überdacht und mit entsprechend angepassten Maßnahmen unterlegt werden.

5. Best Practices: Integration der Private und Public Cloud mit On-Premise-Netzen und -Systemen

Viele Unternehmen haben Cloud Computing in Form von Test- und Probe-Inseln oder alleinstehenden SaaS-Lösungen im Einsatz. Aktuell ist die Herausforderung, Cloud Computing geordnet und skalierbar in die Unternehmens-IT einzubinden.

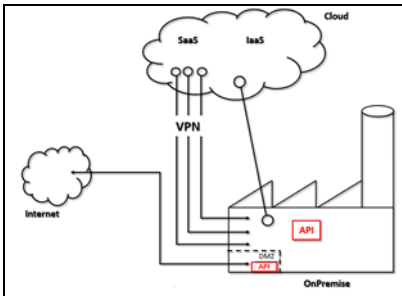
Damit macht es Sinn, die verschiedenen Integrationsmöglichkeiten hinsichtlich einer Best Practise innerhalb der CBA-Lab-Mitgliedsunternehmen zu untersuchen. Best Practices der Cloud-Integration umfassen dabei die Betrachtung der Netz- und Kommunikationsebene, der Applikations- und Serviceintegrationsebene und der Datenebene. Alle Ebenen sind dabei als Abstraktion der verfügbaren Technologien zu verstehen, eine Übersicht über alle verfügbaren Technologien und deren Stärken und Schwächen im Einsatz hätte das Untersuchungsziel unerreichbar gemacht hinsichtlich der benötigten Ressourcen und der hohen Änderungsgeschwindigkeit der heutigen Softwareframeworks. Einen guten Überblick über diese Entwicklungen stellt die Cloud Native Computing Foundation zusammen (http://l.cncf.io).

Die Netz- und Kommunikationsebene

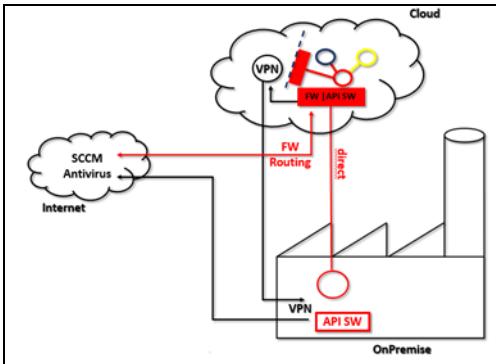


Jede Integration beginnt mit dem osi layer 1, der physikalischen Übertragung. Auch die Cloud-Integration und Network Functions Virtualization (NFV) benötigt weiterhin ein Kabel als Grundlage der Übertragung. Diese Ebene ist, zumeist aus der Historie der Unternehmens-IT, auch der erste Grundschutz für die IT-Sicherheit gewesen. Daher wird bei der Cloud-Integration die Netzwerk-Security weiterhin als Grundelement der IT-Security bei den Teilnehmern betrachtet und durch die unternehmenseigene Netzwerkinfrastruktur und das diesbzgl. Team bereitgestellt. Dabei sind zwei Muster feststellbar: On-Premise Control und Cloud Control.

On-Premise Control

	Die Cloud ist logischer Teil des privaten Netzwerkes des Unternehmens. Zentralistischer Ansatz: jeder Netzwerk-Traffic geht durch eine On-Premise Control. Cloud-Services werden als einzelne „Extensions“ in die On-Premise Network Control eingebunden.
Vorteile	**Nachteile**
Security, Logging, Monitoring ohne Änderungen. Keine cloud-bedingten Transformationsprozesse. Throttling per Cloud-Service möglich. Analysierbarkeit durch zentrale Control.	Mögliche Latenz bei Übergang zwischen unterschiedlichen Services/VPNs. Intermediaries erhöhen die Komplexität zwischen Cloud Services. Netzwerk-Features in Cloud Service (z. B. Security Groups) werden nicht genutzt. Bandbreiten-Management pro Cloud Service notwendig. Peer-to-Peer zwischen Cloud Services nicht möglich. Velocity durch Einsatz von Cloud Services auf Network-Management-Velocity reduziert.

Cloud Control

	Dezentraler Ansatz On-Premise Network Control und Cloud Network Control teilen sich auf. Kürzeste Routen werden möglich, z. B. Cloud-to-Cloud, Cloud-to-Internet, On-Premise-to-Cloud. Service Catalogue dokumentiert die „Position“ im Netz. Abhängigkeitsmanagement.
Vorteile	**Nachteile**
Verfügbarkeit von Service & Daten direkt im gesamten Netzwerk oder in Zonen. Security, Logging, Monitoring als Service nutzbar. Throttling per Service möglich. Peer-to-Peer-Verbindungen zwischen Cloud Service möglich. Nutzung von Network Function Virtualization on Cloud Services direkt möglich.	Mögliche Latenz bei Übergang zwischen unterschiedlichen Clouds. Bandbreiten-Management pro Cloud CSP notwendig und nur noch gesamthaft möglich. Löst nicht sämtliche On-Premise-Verbindungen ab, z. B. Antivirus VPN Service für Desktops. Cloud-bedingte Transformationsprozesse notwendig.

Das von den Teilnehmern gewählte Muster ist dabei von der (IT-)Strategie des Unternehmens abhängig und deren Cloud-Aussagen. Je nach Cloudifizierungsziel werden Mischformen umgesetzt, wobei die Integration mit großen CSP, z. B. MS Azure und AWS, mehrheitlich im Muster Cloud-Control umgesetzt werden, da dort ansonsten zu viel Potential an Network-Automation durch Nutzung der Network-Function-Virtualization-Fähigkeiten der CSP ungenutzt bleiben würde. Diese Fähigkeiten sind durch eine „On-Premise-Schleife" nur schwer nachbildbar.

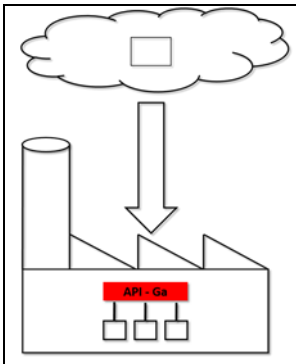
Die Applikations- und Service-Integrationsebene

Die Teilnehmer haben den Umfang der Untersuchung der Applikations- und Serviceintegrationsebene an dem Best Practise der Enterprise Integration Patterns nach dem gleichnamigen Buch des Autors Gregor Hohpe untersucht. Die Betrachtung der 65 genannten Pattern hat allerdings keine Cloud-Spezifika für diese Pattern an sich ergeben. D. h. die Pattern haben weiterhin keine technischen Abhängigkeiten. Allerdings ist die Realisierung der Pattern stark an die von den CSP offerierten Services gebunden, da eine Abweichung von den CSP Services nur durch den Einsatz von Virtual Machine Services (VMs) oder Container Services (Docker/Kubernetes) machbar ist und diese meist teuer im Einsatz sind. Ein Überblick und eine nähere Betrachtung der Unterschiede zwischen den CSP selbst erfolgt im Kapitel 3 Entscheidungshilfe (siehe oben). Dies birgt für alle Teilnehmer allerdings weder ein Risiko noch eine besondere Architekturherausforderung, sodass es keine Best Practices für eine Cloud- und On-Premise-Integration im Spezifischen gibt. Die aktuell existierenden Best Practices zur Integration von Applikationen und Services sind hier daher nicht weiter betrachtet worden.

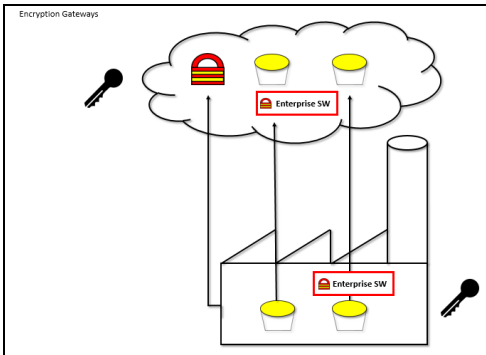
Die Datenebene

Daten, die in der Cloud gespeichert werden, verlassen zu einem gewissen Grad die vollständige Kontrolle der Unternehmen. Daher legt jedes der teilnehmenden Mitgliedsunternehmen auch ein aus der Datensicherheit bestimmtes, unterschiedliches Integrationsziel der Daten an. Typischerweise gibt es immer eine Klasse von Daten, die unter keinen Umständen die volle Kontrolle der Unternehmen verlassen dürfen und diese Daten werden fast ausschließlich On-Premise gehalten und erfahren keine Integration in die Cloud. Für Daten schwächerer Schutzklassen ergeben sich Muster, die neben der vollständigen Integration noch die verschlüsselte Integration und teilweise Integration unterscheiden. Als Basis für die Integration der Datenebene ist eine vorhandene Datenarchitektur immer von Vorteil, da eine operative Cloud-Integration diese nicht ersetzen kann.

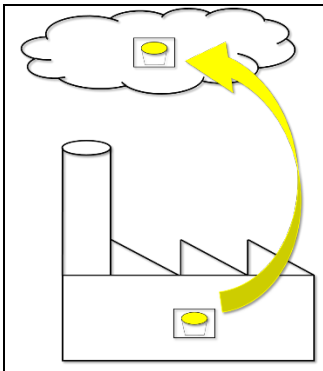
Vollständige Datenintegration

	Transparenter Zugriff auf die On-Premise- und Cloud-Daten. Integrationsarchitektur beschreibt die Infrastruktur für synchronen und asynchronen Zugriff.
Vorteile	**Nachteile**
Vollständige Daten für alle Services und Funktionen nutzbar.	Eingeschränkte Schutzklassen.

Verschlüsselte Datenintegration

	Transparenter Zugriff auf die On-Premise- und Cloud-Daten über Encryption Gateways. Encryption Gateway auch als Service möglich. Integrationsarchitektur beschreibt die Infrastruktur für synchronen und asynchronen Zugriff.
Vorteile	**Nachteile**
Schutzbedürftige Daten können in die Cloud verlagert werden.	Eingeschränkte Schutzklassen. Zusätzlich ein Encryption Gateway (Service) erforderlich. Daten müssen zur Verarbeitung de-crypted werden, dadurch sind meist Analyse- und Reporting-Funktionen eingeschränkt.

Teilweise Integration

	Zugriff auf Cloud-Daten und On-Premise-Daten ist streng getrennt. Cloud-Daten enthalten nur einen Teil der Informationen der On-Premise-Daten. Cloud-Daten sind auf ein Least-to-know für die Funktion reduziert. Integrationsarchitektur beschreibt die Infrastruktur für synchronen und asynchronen Zugriff.
Vorteile	**Nachteile**
Schutzbedürftige Daten können in die Cloud verlagert werden. Cloud-Daten können reduziert werden.	Datenkorrelation zwischen Cloud und On-Premise wird durch getrennte Verarbeitung schwieriger. Datenarchitektur muss Cloud-Daten miterfassen, um diese Daten managebar zu halten.

Unter den Teilnehmern sind alle Muster vorzufinden, der Einsatz richtet sich jeweils nach der Datenarchitektur und/oder den Datenschutzvorgaben.

Der Einsatz von On-Premise- oder Cloud-Integration-Infrastrukturen hat sich bei allen Teilnehmern nach dem Muster des gewählten Netzes und der Kommunikationsebene gerichtet. Damit gestaltet die IT-Strategie der Unternehmen die gewählten Muster. Entscheidende Vor- oder Nachteile, die vorherrschende Muster obsolet oder attraktiv werden lassen, konnten die Teilnehmer nicht feststellen. Damit ist es vorrangig wichtig, eine Cloud-Strategie festzulegen und die Architektur für die eigene Unternehmens-IT-Landschaft zu beherrschen, um den optimalen Weg in die Cloud für sein Unternehmen zu finden. Das Fehlen einer Cloud-Strategie führt zu einem unkontrollierten Einsatz aller vorhandenen Muster, solch geschaffene Komplexität ist durch Architektur zwar erfassbar, aber kaum transformierbar.

Das Fazit der Best Practices für die Cloud- und On-Premise-Integration ist daher eine Umsetzung der Cloud-Strategie und der Reduzierung der implementierten Muster im eigenen Unternehmen.

6. Fazit und Ausblick

Eine Multi-Cloud-Strategie ist für die Innovationskraft im Unternehmen und das Ermöglichen einer unterstützenden IT keine Wahlmöglichkeit mehr für die Unternehmen. Die im Austausch der Mitglieder gefundenen Erfahrungen und Muster bei der Umsetzung liefern für die eigene Strategie und deren Umsetzung wertvolle Hinweise. Dabei gilt es, vom eigenen Standpunkt den besten Weg zum Ziel der Unternehmensstrategie zu definieren und ihm zu folgen. Unter den vielen Wegen gibt es gut beschrittene Pfade, die zeigen, dass individuelle Wege heute keine Vorteile mehr bieten.

Die Menge an Multi-Cloud für das eigene Unternehmen sollte immer übersichtlich bleiben, die Angebote an Funktionen sind, über die Zeit gesehen, bisher bei allen Cloud Service Providern nicht stark differenzierend. Dies gilt ins Besondere für die grundlegenden Funktionen und Dienste, sodass eine Auswahl an CSP durchaus nach den besonders benötigten Stärken eines CSP erfolgen sollten. Die Grundleistungen der CSP werden immer austauschbarer werden, sodass eine cloud-agnostische Entwicklung von Unternehmensapplikationen im Vorhinein mehr Aufwände als Nutzen bringt. Die gerade im Markt beginnende Etablierung von Cloud-Broker-Lösungen, wie Google mit Anthos dies gerade startet, zeigt, dass die CSP hier selbst für Austauschbarkeit sorgen werden. Dies legt nahe, bei der CSP-Auswahl auf eine Differenzierung deren Stärken zu achten. Suchen Sie als Unternehmen daher zwei unterstützende CSP als Partner ihrer Unternehmens-IT, um ihre Innovationskraft durch schnelle IT-Funktionen und -Unterstützung zu sichern.

Eine Einbindung des CSP nehmen Sie nach Ihrem Sicherheits- und Risikobewusstsein vor. Dabei legen Sie Ihre Erfahrungen aus bisherigen Cloud-Anbindungen zugrunde und entscheiden eine nachhaltige Integrationsstrategie. Nur **keine** Strategie wird Sie am Ende mehr Geld und Zeit kosten, da die Integrationsvielfalt Ihre Ressourcen binden wird. Das Unternehmen wird langfristig auf die Cloud-Kraft nicht verzichten können und wollen.

7. Literaturverzeichnis

https://aws.amazon.com/de/architecture/well-architected/

https://www.computerwoche.de/a/wie-sich-die-grossen-cloud-trends-entwickeln,3546147