Planerische Schwerpunkte Hybrider IT-Konzepte

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Dr. Roman Bansen | Bitkom e. V.
T 030 27576-270 | r.bansen@bitkom.org

Verantwortliches Bitkom-Gremium

AK Hybride IT

Autoren

Thore Bahr | SUSE Software Solutions Germany GmbH
Dr. Roman Bansen | Bitkom e. V.
Frank Beckereit | NTT Germany AG & Co. KG
Martin Beuse | Hewlett-Packard GmbH
Stefan Böhler | Microsoft Deutschland GmbH
Peter Dümig | Dell GmbH
Sven Kaminski | SVA System Vertrieb Alexander GmbH
Roman Kempter | T-Systems Multimedia Solutions GmbH
Andreas Landenberger | iSAQB e. V.
Jürgen Lang | IBM Deutschland GmbH
Arne Lehfeldt | Dell GmbH
Klaas Mertens | Equinix (Germany) GmbH
Holger Nicolay | Interxion Deutschland GmbH
Volker Niedermeier | Fujitsu Technology Solutions GmbH
Dr. Markus Platz | Insentis GmbH
Rui Manuel Tavares | Fujitsu Technology Solutions GmbH

Titelbild

© Sami Anas – pexels.com

Inhaltsverzeichnis

Einleitung

Heutige Anforderungen von Unternehmen an ihre IT-Umgebungen sind häufig nicht mehr nur durch unternehmenseigene Rechenzentren oder nur durch (Cloud-) Provider-Angebote zu bewältigen. Unternehmen nutzen vielmehr die Vorteile verschiedener IT-Welten, beziehen ihre Services sowohl vom eigenen (On-Premises-) Rechenzentrum, als auch von Dritten wie Hosting-, Housing-, Outsourcing- oder Public-Cloud-Providern.

In einer solchen Hybriden IT werden Services sowohl selbst erbracht als auch von Dienstleistern bereitgestellt gestellt (»Make and Buy«). Durch diese Kombination gelten viele altbekannte Regeln des bisherigen lokalen IT-Betriebs weiter, es kommen aber auch solche hinzu, die sich aus der Zusammenarbeit mit externen Dienstleistern ergeben. Diese Regeln der On-Premises- und der Dienstleister-Welt können aber nicht eins-zu-eins übertragen werden. Sie müssen vielmehr überarbeitet und auch ergänzt werden, um zu einer vollständigen Ende-zu-Ende-Abdeckung zu gelangen.

Im vorliegenden Dokument hat der Arbeitskreis Hybride IT im Bitkom e.V. diejenigen Aspekte heraus gearbeitet, denen nach Ansicht der Autoren bei der Planung und Umsetzung einer Hybriden IT besondere Aufmerksamkeit geschenkt werden sollte. Es geht um die Hybrid-IT-spezifischen Zusätze, die auf der Basis der klassischen IT notwendig sind.

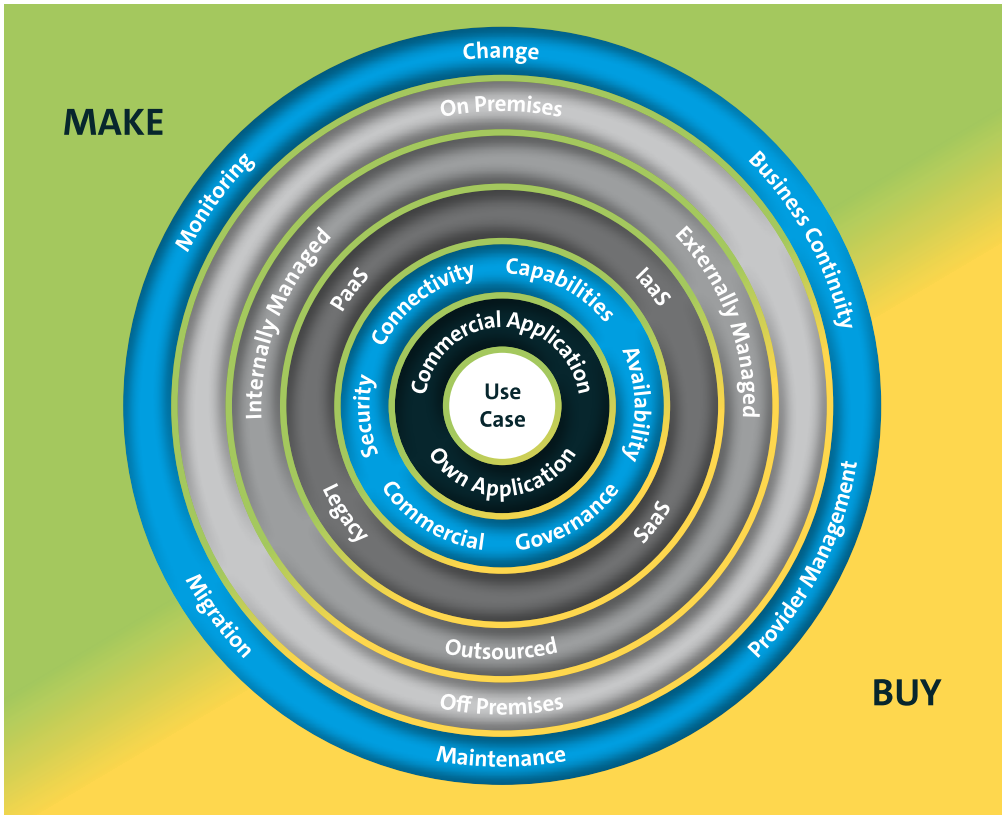
Hierbei handelt es sich vornehmlich um Querschnittsfunktionen und diejenigen Begriffe, die im untenstehenden Schaubild in den blauen Ringen angeordnet sind. Dies sind häufig nicht nur rein technische, sondern vor allem organisatorische Aspekte, denen in der Hybriden IT eine besondere planerische Aufmerksamkeit zukommen sollte.

Das vorliegende Dokument knüpft dabei nahtlos an die vorherige Publikation des Arbeitskreises Hybride IT an, das Whitepaper Grundlagen, Definition & Glossar. In diesem wird der Leser mit der Idee des untenstehenden Schaubildes vertraut gemacht, das die – nach Ansicht des Arbeitskreises – unabdingbar notwendigen Schritte zur Planung Hybrider IT grafisch beschreibt. Zweiter Bestandteil des Dokuments ist ein Glossar, das zahlreiche Begrifflichkeiten definiert, die für ein gemeinsames Verständnis der Herausforderungen und der Lösungsansätze im Zusammenhang mit Hybrider IT notwendig sind.

Sie finden das Dokument »Hybride IT – Whitepaper: Grundlagen, Definition & Glossar« des Bitkom Arbeitskreises Hybride IT unter der folgenden Adresse zum Download:
↗https://www.bitkom.org/Whitepaper_Hybride_IT

Die Inhalte sind zudem auch direkt auf der entsprechenden Webseite des Bitkom abrufbar:
↗https://www.bitkom.org/Hybride-IT

Um dem Leser die Vertiefung der beschriebenen Aspekte zu erleichtern, enthalten die nachfolgenden Kapitel zahlreiche Links zu weiterführenden Publikationen. Diese wurden zum Zeitpunkt der Veröffentlichung auf Korrektheit überprüft, deren Funktionieren kann aber leider nicht für alle Zukunft sichergestellt werden. Zudem ist zu betonen, dass diese externen Verweise auf weiterführende Literatur und Quellen verweisen, die nach Ansicht der Autoren lesenswert sind, die dort veröffentlichten Aspekte und Bewertungen aber nicht vollständig die Meinung des Arbeitskreises Hybride IT im Bitkom e.V. widerspiegeln müssen.



Blaue Kreise in der Grafik: ○ → **Erhöhte planerische Relevanz bei Hybrider IT**

Abbildung 1: Die Grafik verdeutlicht die unterschiedlichen Aspekte, die bei der Auswahl und Planung von Anwendungen und Services in Hybrider IT zu beachten sind. Beginnend mit dem Use Case ist das Schaubild von innen nach außen zu lesen, um ein umfassendes Bild der Hybriden IT als Ganzes zu vermitteln. Die im Rahmen dieses Leitfadens behandelten planerischen Schwerpunkte finden sich in den zwei blauen Kreisen wieder.

1 Security

1 Security

Ein bestehendes aktuelles IT-Security-Konzept bzw. ein vorhandenes IT-Sicherheitsmanagement für On-Premises Data-Center-Umgebungen bildet eine mögliche Grundlage für eine Erweiterung dieser Sicherheitskonzepte um hybride Anwendungsszenarien. Hierbei gilt zu prüfen, ob das bestehende IT-Sicherheitskonzept aktuell ist und auf dem neuesten Stand der Risikovermeidung entwickelt wurde.

Durch eine hybride Anwendungswelt entstehen neue Angriffspunkte, Gefahren und Bedrohungen für die IT-Sicherheit. Datenintegrität, Vertraulichkeit, Identitätssicherheiten oder auch Datenauthentizität sind nur einige Beispiele, die es hier zu betrachten und bzgl. Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe zu bewerten gilt.

Alle Kapitel der IT-Sicherheit sind auf die angepassten hybriden Konzepte zu überprüfen und neue Gefahren oder Bedrohungsszenarien zu analysieren. Hierzu zählen neue oder veränderte Rollenmodelle, Berechtigungsstrukturen, Policies, Verschlüsselungskonzepte, Softwareentwicklung, Netzwerksegmentierungen, Intrusion Detection, Zertifikatsmanagement, Lizenzmanagement und vieles mehr.

Besondere Bedeutung kommt hier dem Risikomanagement bzw. der Risikoanalyse zu. Durch eine sehr frühzeitige Risikoanalyse von Laufzeitumgebungen und Workflow-Prozessen können mögliche Schwachstellen, Bedrohungen und Angriffspunkte entdeckt und ermittelt werden. Diese Erkenntnisse können helfen, erweiterte Sicherheitskonzepte für hybride Umgebungen zu schaffen und auch erfolgreich umzusetzen.

Vorarbeiten zu den Bereich Security im Bereich On-Premises bzw. Security und Cloud sind bereits hinreichend durch das Bundesamt für Sicherheit in der Informatik erarbeitet und veröffentlicht worden. Sie beschreiben Vorgehensweisen und Methoden zum Umgang mit Security.

- **↗BSI-Standard 200-1: Managementsysteme für Informationssicherheit**
- **↗BSI-Standard 200-2: IT-Grundschutz-Methodik**
- **↗BSI-Standard 200-3: Risikomanagement**
- **↗Leitfaden Basis-Absicherung**
- **↗BSI-Standards 100-1, 100-2, 100-3**
- **↗BSI-Standard 100-4: Notfallmanagement**
- **↗BSI C5 (Kriterienkatalog *Cloud Computing Compliance Criteria Catalogue* C5)**
- Die ISi-Reihe (BSI-Standards zur Internet-Sicherheit) gibt konkrete technische Empfehlungen zu verschiedenen Themenbereichen der IT-Sicherheit.

Was ist neu am Thema Security unter Hybrider IT?

Während alle bisher beschriebenen Hinweise sehr genau das Thema Security für die On- bzw. Off-Premises Welt beschreiben, vermischt sich diese klare Trennlinie bei Hybrider IT. Benötigt wird ein auf die Use Cases anwendbares Security Framework, was der Agilität der Verschiebbarkeit zwischen On-Premises und Cloudwelt gerecht wird. Es kommt zu einer Verzahnung der beiden Welten.

Die Erstellung eines durchgängigen Security-Konzeptes ist zum Beginn des Weges zu Hybrid-IT unerlässlich und dessen Planung muss einen angemessenen Raum einnehmen. Hierbei sind sämtliche Bereiche, in denen Security eine Rolle spielt, zu beachten. Angefangen bei der Authentifizierung und Zugriffsteuerung, welches sich in einem schlüssigen Benutzerkonzept abbilden muss, über passive Sicherungsmechanismen wie Firewalls, Endpoint Protection und Verschlüsselung bis hin zu aktiven Maßnahmen wie IDS (Intrusion Detection System) und IPS (Intrusion Prevention System).

Themen wie »Wie identifiziere ich bekannte Geräte und Benutzer?« und »Wie gehe ich mit unbekannten Geräten um?« müssen ebenfalls Beachtung finden. Die Implementierung von den Anforderungen angemessenen Identitäts-Management-Applikationen ist unumgänglich.

Die Security darf darüber hinaus nicht schon am Client oder Server enden, sondern geht bis in die Applikation oder den Container.

Die Benutzung von Tools, die die Sicherheitsregeln und die Schutzmechanismen automatisch ausrollen und sowohl On-Premises und Off-Premises einheitlich sicherstellen, werden unerlässlich, um die Komplexität zu bewältigen und die Fehleranfälligkeit zu minimieren. Dieses bildet auch die Basis, um Workloads einfacher zwischen On-Premises und Off-Premises hin und her zubewegen. Das Regelwerk muss sowohl für On-Premises als auch für Off-Premises schlüssig und konsistent sein.

Einheitliche Tools für On-Premises und Off-Premises bieten hier große Vorteile. Es darf beim Wechsel von On-Premises zu Off-Premises oder umgekehrt nicht zu einem Bruch in der Tool-Landschaft kommen.

Diese neuen Tools müssen auch das Change Management und das Update- und Patchverfahren in der gesamten Hybriden IT automatisieren und vereinheitlichen können.

Grundsätzlich muss der Anteil der automatisch durchführbaren Aufgaben signifikant gesteigert werden. Ein Großteil des heutigen Aufwandes in der Administration entfällt auf die manuelle Umsetzung von Änderungen oder Konfigurationen des Netzwerkes bzw. der Sicherheitsgeräte. Neben der Verhinderung von menschlichen Fehlern wird die Automatisierung Ressourcen in der IT-Mannschaft freisetzen, die für Optimierung der IT-Landschaft und zukünftige Innovationen genutzt werden können.

Für das Controlling der Sicherheitsmaßnahmen werden neben den auditsicheren Verfahren und dem sicheren Verwahren der Logfiles auch einfache Dashboards benötigt, die den gesamten Security-Pfad Ende-zu-Ende darstellen können. Die Sichtbarkeit des Regelwerks muss einfach sein. Die Reaktionen auf mögliche Angriffe müssen vollautomatisiert werden

Die im Security-Konzept zu berücksichtigende Microsegmentierung stellt ein mächtiges Werkzeug dar. Im Falle des Erkennens eines Angriffs können die entsprechenden befallenen Geräte, virtuellen Maschinen oder Applikationen bzw. Container schnell in Quarantänezonen gebracht und weitere Schäden vermieden werden. Der mögliche Befall hat ggf. nur sehr kleine Bereiche betroffen.

Für die aktive Sicherung sollten IDS- bzw. IPS-Systeme eingeführt werden. Intrusion Detection Systems analysieren den Netzwerkverkehr im Hinblick auf Signaturen, die mit bekannten Cyber-Angriffen übereinstimmen. Intrusion Prevention Systems führen auch eine Paketanalyse durch, können aber je nach erkanntem Angriffstyp zudem die Auslieferung des Pakets verhindern – und so den Angriff stoppen.

Wenn Daten in der Cloud liegen sollen, muss über starke Verschlüsselung nachgedacht werden und diese dann auch implementiert werden.

Alles in allem sind die Anforderungen an Security bzgl. Hybrid-IT nicht signifikant anders, als wenn man ausschließlich lokal implementiert. Die IT-Landschaft wird nur größer und komplexer. Dies kann allerdings mit durchdachter Konzeptionierung und Planung sowie den richtigen Tools gemanagt werden.

Die Konzepte sollten vor allem durchgehend sein, so dass z.B. eine Regel, die eingehende Verbindungen für einen Service aus dem Internet On-Premises untersagt, nicht in der Public Cloud zulässig sein oder umgekehrt.

Die Hyperscaler bieten bereits sehr hohe Schutzmaßnahmen gegen breit gerichtete Angriffe. Was allerdings im Umkehrschluss nicht bedeutet, dass per se alles abgesichert ist. Es bedarf weiterhin eines guten Security-Konzeptes und dessen Umsetzung. Sonst könnte z.B. ein Objekt-Speicher öffentlich zugänglich sein, der sensible Daten enthält, nur weil er fälschlicherweise so konfiguriert wurde. Auch gibt es bei modernen Cloud-Applikationen große Unterschiede in der Architektur im Vergleich zu (monolithischen) Legacy-Anwendungen, die andere Security-Konzepte benötigen. (Access) Keys dürfen nicht in Repositories abgelegt werden, Buckets oder Serverless-Funktionen müssen unbedingt eine Autorisierung abfragen, um nur zwei Beispiele zu nennen, die in klassischen Anwendungen normalerweise nicht zum Tragen kommen.

Durch die Verwendung von neuen Services entstehen auch Vorteile, so hat Microsoft zum Beispiel bei der Authentifizierung in der Cloud, ältere und wenig sichere Varianten gestrichen, die On-Premises aber noch zum Einsatz kommen. Es gibt aber auch viele Themen, die On-Premises und in der Cloud gleichermaßen umgesetzt werden müssen, wie zum Beispiel die Trennung von Audit-Daten und -Accounts von anderen administrativen Zugängen. Bei der Nutzung der

Cloud muss das Shared Responsibility Model konsequent umgesetzt werden. Hierbei ist der Anbieter für die Sicherheit seiner Infrastruktur zuständig und der Nutzer für die Sicherheitskonfiguration.

Durch die Public Cloud haben auch Fachabteilungen in den Unternehmen die Möglichkeit, an der zentralen IT vorbei Services zu beziehen und aufzubauen. Dies hat in den vergangenen Jahren deutlich zugenommen und wird unter dem Begriff Schatten-IT deklariert. Hier besteht insbesondere das Risiko, dass nicht fachkundiges Personal gravierende Sicherheitslücken im Zugriff auf sensible Daten erzeugt, etwa Personaldaten öffentlich in einem Cloudspeicher abzulegen, um nur ein einfaches Beispiel zu nennen. Zur Erkennung der Nutzung von Public-Cloud-Diensten haben Security Anbieter bereits Produkte entwickelt, mit denen IT-Abteilungen Analysen hierzu erstellen können. Ein anderer Weg ist, auch die Buchhaltungs- und Reisekosten-Abteilung einzubeziehen, da hierüber die Auslagen für die Schatten-IT entsprechend abgerechnet und damit rückverfolgt werden können.

2 Connectivity

2 Connectivity

Ein besonderes Augenmerk gilt es auf die Netzwerkanbindung zu legen, wenn Applikationen ganz oder teilweise zu Service-Providern oder in Public Clouds verlagert werden. Neben der technischen gilt es in vielen Unternehmen, zusätzlich eine organisatorische Herausforderung, die klassische Trennung zwischen IT- und Netzwerk-Abteilung, zu bewältigen.

Sollen Public-Cloud-Provider als Teil der hybriden IT integriert werden, so verstehen diese unter »Cloud Networking« die Einbindung und Nutzung ihrer eigenen, Cloud-basiert bereit gestellten Netzwerk-Services wie Firewall- oder Content-Distribution-Services, sowie die Verbindung und Trennung einzelner Cloud-Instanzen mittels Gateways. Solche Netzwerke innerhalb einer Cloud-Umgebung lassen sich üblicherweise durch wenige Zeilen Code oder per Mausklick und weitgehend ohne technische Limitierungen konfigurieren, sofern der Anwender sich sowohl auf die Netzwerk- als auch auf die Cloud-Konfiguration versteht.

Zu beachten ist jedoch, dass Public Cloud Provider, Hosting Provider und Managed Service Provider ihre Dienste – im Unterschied zu klassischen Applikationen im eigenen Unternehmensrechenzentrum – oftmals aus Infrastrukturen heraus erbringen, die sich außerhalb der lokalen Netzwerkgrenzen befinden. Die Netzwerkverbindung an diese Dienste ist daher essenziell, weil mit der räumlichen Distanz zwischen den Applikationen im Provider-Rechenzentrum und den Applikationen oder Daten in eigenen Räumen die Latenz (Signallaufzeit) steigt, was sich negativ auf die Performance des Gesamtsystems auswirken kann.

Für die Anbindung von Nutzern beziehungsweise Arbeitsplätzen an Public-Cloud- oder Service-Provider-Infrastrukturen wird üblicherweise das öffentliche Internet genutzt. Hierbei ist aus Gründen der Performance zu beachten, wie die Anbindung der Provider-Infrastruktur an das öffentliche Internet, die Verbindungen der Internet-Service-Provider (ISPs) untereinander und die Anbindung der einzelnen Nutzer an das Internet erfolgt.

Beim Netzwerkkonzept für große Standorte mit zahlreichen Nutzern (wie beispielsweise einer Unternehmenszentrale) spielt es zudem eine wichtige Rolle, ob die Internet-Anbindung – in Abhängigkeit von der Glasfaser-Verfügbarkeit vor Ort – breitbandig und redundant ausgeführt werden kann. Zudem ist zu beachten, dass gehostete oder in einer Public Cloud betriebene Business-Anwendungen je nach Use Case in einem symmetrischen Datenfluss resultieren können (Up- und Downstream ähnlich groß), anders als es beispielsweise beim Streamen von Filmen der Fall ist.

Eine Möglichkeit, die Unzulänglichkeiten des öffentlichen Internet zu umgehen ist – gerade im Fall von großen oder unternehmenskritischen Standorten – die Anbindung über private und dedizierte Verbindungen. Solche Datenleitungen werden von einem Telekommunikationsanbieter direkt vom Kundenstandort an die Übergabepunkte der Cloud- bzw. Managed-Service-Provider-Infrastruktur geführt.

Neben der Anbindung der Nutzer an die Provider-Infrastruktur gilt es bei der Hybriden IT zu beachten, dass der überwiegende Datenverkehr nicht zwischen Anwender und Applikation, sondern zwischen auf verschiedene Standorte verteilten Applikationen entsteht. Laut des regelmäßig erhobenen Cisco-Cloud-Index macht dies 70 % bis 80 % des gesamten Netzwerkverkehrs aus.

Hierbei spielt die physische Lokation der genutzten Service-Provider- oder Public-Cloud-Applikation eine gewichtige Rolle. Der Unterschied in der Signallaufzeit innerhalb des eigenen Rechenzentrums ist im Gegensatz zu einer in Deutschland (beispielsweise in Frankfurt) oder auch Zentraleuropa (Amsterdam) bereit gestellten Provider-Applikation allein schon durch die räumliche Distanz enorm. Hinzu kommen die zu erwartenden Bandbreitenschwankungen, sofern die Datenpakete zwischen dem eigenen Unternehmensrechenzentrum und dem Provider über die Netzinfrastrukturen mehrerer Internet-Service-Provider geschickt werden müssen.

Eine mögliche Lösung dieser Problematik – gerade im Umfeld von hybriden IT-Infrastrukturen – ist die Nutzung von solchen Colocation-Angeboten, bei denen die eigenen IT-Applikationen in direkter räumlicher Nähe, quasi Tür-an-Tür im selben Rechenzentrum, zum genutzten Managed-Service-Provider oder den großen Public-Cloud-Anbietern betrieben werden können. So lassen sich Datendurchsatz und Signallaufzeit zwischen eigenen und zugekauften Anwendungsteilen so optimieren, dass diese wieder annähernd denjenigen im eigenen Rechenzentrum entsprechen. Auch viele Hosting- und Managed-Service-Provider bedienen sich der Basis-Infrastruktur führender Colocation-Provider, so dass auch hier durch die Verlagerung des »On-Premises«-Teils der Hybriden IT vom Unternehmensrechenzentrum weg hin in die Colocation Performanz- und Kostengewinne im Netzwerkbereich zu erzielen sind.

Zusammenfassend gilt es, Mittel und Wege zu finden, die Verkehrsströme in zukünftigen hybriden IT-Umgebungen im Vorhinein zu analysieren und die Netzwerk-Optimierung als Teil des Planungs- und Migrationsprojektes durchzuführen.

Die Nutzung von privaten Netzen zur Anbindung von Applikationsteilen untereinander ist in vielen Fällen – im Gegensatz zur Anbindung der Anwender – aus Verfügbarkeits- und Kostengründen oftmals angeraten, zumal eine solche Verbindung von Applikationsinfrastrukturen untereinander weitere Vorteile in Bezug auf den Datenschutz und die IT-Sicherheit mit sich bringt.

Diese Entscheidung für ein hybrides Szenario muss die drei Dimensionen

- Service-Verfügbarkeit von IT- und Netzwerkinfrastruktur (technisch),
- Gesamtpreis für den IT- und den Netzwerkbetrieb (kommerziell) sowie
- die räumliche Distanz zum eigenen Rechenzentrum aus Netzwerkperspektive berücksichtigen.

Netzwerkseitig bieten sich folgende Lösungsmöglichkeiten an:

- Für die Anbindung der User ist meist das öffentliche Internet geeignet.
- Die Verbindung der unterschiedlichen Applikations-Infrastrukturen untereinander sollte je nach Anforderung über Verbindungen mit möglichst wenigen Netzübergängen erfolgen.
- Distanzen und damit Netzwerkprobleme können überwunden werden, indem Colocation-Services für eigene Infrastrukturen in Erwägung gezogen werden, sofern diese bei genau demjenigen Anbieter genutzt werden, der auch das IT-Service-Provider-Rechenzentrum oder die genutzten Public-Cloud-Services beheimatet.

3 Capabilities

3 Capabilities

Die größte Herausforderung, welche die Hybride IT mit sich bringt, ist die Komplexität. Diese betrifft nicht nur die Technik, sondern auch Prozesse, und stellt vor allem neue Anforderungen an die Fähigkeiten und Fertigkeiten der Mitarbeiter. Daher sollte ein Unternehmen sicherstellen, dass es über die notwendigen Kompetenzen in Bezug auf das Personal und die nötigen Tools sowie in Bezug auf die Infrastruktur zum erfolgreichen Management der Komplexität verfügt.

Kompetenzen

Das Management (bspw. CIO) sollte sich mit den folgenden Aspekten vertraut machen, um den komplexen Anforderungen von hybriden Infrastrukturen gerecht zu werden und hybride IT Landschaften erfolgreich im Unternehmen implementieren zu können:

- Umgang mit Komplexität in der Führungsverantwortung
- Wirtschaftliche und Datenplanungsmodelle
- Einführung entsprechender Kontroll-/Überwachungsmechanismen. Dies erfordert die Kenntnis über hybride IT-Überwachungstools zur Transparenz des gesamten Stacks.
- Sicherstellen der nötigen Kompetenzen in Teams durch Zusammenführung der Experten aus den benötigten Fachrichtungen.
- Aufbau von Communities, die den Wissensaustausch der verschiedenen Fachrichtungen befördern.
- Fortlaufende Einbindung von Entscheidern, um fortlaufend die Übereinstimmung mit der Business- und IT-Strategie sicherzustellen.

Insbesondere die Funktionen Ingenieure und Solution-Architekten müssen neue Kompetenzen ausbilden, um mit den hohen Anforderungen hybrider IT-Landschaften gewachsen zu sein.

- Fortlaufende Qualifizierung zu den genutzten Kerntechnologien
- Umfangreiches Wissen zu Prinzipien im Cloudumfeld und den genutzten Plattformen
- Ende-zu-Ende-Überwachungs- und Verwaltungstools
- verteilte Anwendungsarchitektur und deren Implikationen
- Prozessautomatisierungen über Applikationen und Plattformen hinweg
- Datenanalyse und Big Data
- Enge interdisziplinäre Zusammenarbeit über Strukturgrenzen hinweg zur Sicherstellung der Service Level in den gesamten Applikationsketten
- Business-Continuity-Management und Implementierung von auf die verteilten Systeme ausgerichteten Service-Strukturen.

Prozesse

- Verteilter Betrieb bedeutet auch, getrennte Verantwortung und Verantwortungsübergänge. Diese müssen im Vorfeld geklärt werden und können durchaus was z.B. SLA angeht unterschiedlich interpretiert werden.
- Auch wenn im Normalfall der Cloudanbieter die Ressourcen ohne vorab Bestellung zur Verfügung stellen kann, ist eine verteilte Kapazitätsplanung notwendig, denn Ressourcen die On-Premises bereitgestellt werden müssen, bedürfen der eigenen Planung und Beschaffung.
- Kommunikationsstrukturen zwischen den einzelnen Providern sind im Vorfeld zu definieren um im Fehlerfalle, kurze Eskalationswege sicherstellen zu können.
- Ständige Optimierungsprozesse in Bezug auf Technologien und Kosten. Es muss im Prozess definiert werden wie ein Unternehmen von den ständigen Verbesserungen partizipieren kann.
- Verteiltes Monitoring, welche Schnittstellen werden seitens des Dienstleisters zur Verfügung gestellt und wie können diese in die bestehenden Prozesse eingebunden werden.
- Es muss ein Prozess zur nutzungsgerechten Abrechnung von Diensten etabliert werden. Hier bei ist es wichtig, dass die Kosten nicht statisch sind, somit auch eine Budgetierung im Vorfeld schwer abzuschätzen ist. Alternativen bieten hier Kosten Management Tools der Cloudanbieter oder auch als Zukauf von Drittanbietern.

Tools

Bei der Arbeit in hybrider Infrastruktur ist nicht nur kompetentes Personal essenziell, es müssen auch Tools und Strukturen vorhanden sein, um die komplexen Anwendungen monitoren und steuern zu können:

- Zentraler Überblick über Vor-Ort- und Cloudumgebungen: einsatzbereites und umfassendes Tool-Set zum Zustands- und Performance-Monitoring
- Tools, welche Zeitreihendaten zusammenführen und korrelieren, zur Darstellung und Analyse der gesamten Systemlandschaft
- einheitliche Konfigurations-, Patch- und Update-Automatisierungen im Hinblick auf Applikation, Middleware und Infrastruktursoftware
- fortschrittliche Analyseverfahren für Kapazitätsplanung sowie Performanceoptimierung
- Bereitstellung von Datensicherungs- und Rücksicherungslösungen
- Lösungen zur einheitlichen und konsistenten Rechteverwaltung
- Integration mit vorhandenen Systemen und Management-Tools
- Implementierung von Standardprozessen für die Elemente der Service-Kataloge
- Tools für systemweite Qualitäts- und Zuverlässigkeitstests von Anwendungen

Quellen

↗https://www.pcwelt.de/a/hybride-it-die-drei-groessten-herausforderungen,3450134
↗https://www.cloudcomputing-insider.de/hybride-it-infrastrukturen-erfolgreich-orchestrieren-a-845667/
↗https://www.computerwoche.de/a/ein-neues-management-fuer-eine-hybride-it,3212140
↗https://www.netzwoche.ch/news/2019-05-20/strategien-fuer-eine-hybride-it-architektur
↗https://www.channelpartner.de/a/voraussetzungen-fuer-eine-erfolgreiche-hybride-it-infrastruktur,3335956
↗https://www.solarwinds.com/company/press-releases/solarwinds-it-trends-report-2017-portrait-of-a-hybrid-it-organization-finds-german-it-realizing-cost

4 Availability

4 Availability

Definition

Availability (dt. etwa »Verfügbarkeit«) bezeichnet die Verfügbarkeit von Programmen oder Systemen über die Zeit. IT-Systeme und Services sind ihrer Natur nach nie fehlerfrei und müssen gewartet werden, können aber auch ungeplant ausfallen. Availability befasst sich mit technischen und prozessualen Vorkehrungen, um die IT-Systeme für das Unternehmen benutzbar zu halten und im Fehlerfall schnellstmöglich diese wiederherzustellen.

Metriken

Die Availability wird in Prozent einer definierten Zeitspanne angegeben. Z.B. bedeuten 99,5 % über 24 h × 365 Tage/Jahr, dass der betreffende Service knapp 1,9 Tage pro Jahr ausfallen darf und dennoch seine Verfügbarkeitsanforderungen erfüllen würde.

Üblich sind bei wichtigen Systemen Verfügbarkeiten von 99,9 – 99,999 %, wobei höhere Zahlen auch aufwendigere Architekturen und meist deutlich höhere Kosten bedeuten.

Die Definition, wann ein Service als »verfügbar« gilt, muss dabei unbedingt klar im Vorfeld definiert werden. Dies kann im Einzelfall die generelle Erreichbarkeit eines Servers sein, aber auch ein Geschwindigkeitsfaktor (z.B. Transaktionen pro Sekunde) oder die Verfügbarkeit von spezifischen Funktionen eines Dienstes. Erfahrungsgemäß sind hier die Sichtweisen auf On-Premises und Cloudleistungen durchaus unterschiedlich und können im schlechtesten Fall die Erwartungshaltung verfehlen.

SLA und OLA

Mit der Einführung von ITIL wurden die Begriffe SLA (Service Level Agreement) und OLA (Operational Level Agreement) eingeführt. Diese beschreiben die Anforderungen an die Qualität eines Service, seine Leistungs- und Verfügbarkeitsanforderungen sowie zugeordneten Pönalen, sofern die Services nicht definitionsgemäß erbracht werden.

SLA definieren dabei die Anforderungen an einen Service, während OLA die Leistungen von zu liefernden Einheiten beschreiben. Speziell im Outsourcing ist die Availability ein wichtiges Kriterium in der Spezifikation der Leistungserwartung zwischen den Parteien.

Pönalen

Üblicherweise werden Abweichungen von vereinbarten Verfügbarkeiten mit Pönalen durch die Vertragspartner belegt. Da bei Systemen, die nicht ausreichend verfügbar sind, dem Unternehmen (oder Kunden) wirtschaftliche Nachteile entstehen, sollen die Pönalen den Leistungserbringer dazu motivieren, seine Leistungsfähigkeit sicher zu stellen. Daher sind Pönalen so zu wählen,

dass eine nicht ausreichende Vorsorge beim Leistungserbringer für diesen im Fehlerfall teurer werden muss, als wenn er die Verfügbarkeit sicherstellen würde.

Anwendbarkeit

Verfügbarkeiten werden sinnvollerweise immer Ende zu Ende gemessen, was bei hybriden Umgebungen manchmal schwierig sein kann. Die gesamte Verfügbarkeit einer Lösung liegt dabei immer unter der Verfügbarkeit der einzelnen Komponenten. Daher müssen die Bestandteile einer Lösung immer gesamtheitlich berechnet werden, um die gewünschte Verfügbarkeit des Gesamtsystems sicher zu stellen.

Speziell Cloudangebote bieten häufig keine allzu hohen Verfügbarkeiten an oder sie sind nicht transparent im Hinblick auf die darunterliegende, technische Architektur. Hier ist die Auswahl des passenden Angebots sowie die Integration in den On-Premises-Teil fundiert zu planen und auf Tauglichkeit zu prüfen. Ebenso werden für viele SaaS-Angebote nur unzureichende Datensicherungslösungen angeboten, weshalb auch hierauf entsprechendes Augenmerk gelegt werden sollte.

5 Governance

5 Governance

Governance-Aspekte sollten während der Vertragsverhandlungen mit dem Anbieter von Cloud-Infrastrukturen und somit vor der Migration in eine hybride Umgebung berücksichtigt werden. Im Fokus stehen hier Zugangsrechte, Prüfrechte, sowie weitere Regelungen zu rechtlichen Rahmenbedingungen.

Abrechnung

Abrechnungsmodelle in hybriden Infrastrukturen sollten Kostenschwankungen abbilden können. Wenn es zur Entscheidung kommt, wo ein Service betrieben werden soll, muss unter anderem auch der aktuelle Preis bzw. die Kosten als Entscheidungskriterium mit herangezogen werden können.

Rechtliche Aspekte

Eine Verpflichtung des Service-Anbieters, geltende Normen und Gesetze in Abhängigkeit des Standortes und der relevanten Branche einzuhalten, sind hier die Grundvoraussetzungen. Weiterhin bleibt aber das beauftragende Unternehmen verantwortlich im rechtlichen Sinne.

Ziel sollte daher sein, dass die Leistungen, die durch die Einbindung weiterer Infrastrukturen erbracht werden, transparent gegenüber dem nachweis- und dokumentationspflichtigen Unternehmen sind.

Zudem ist vertraglich zu regeln, dass Sicherheitsrichtlinien und Kontrollen auch von Dritten angewendet werden dürfen. Im Hinblick auf eine mögliche Beendigung der Nutzung sind Vereinbarungen zu treffen: Kündigungsregelungen, Vertraulichkeitsvereinbarungen, Vereinbarung von Vertragsstrafen, Festlegung von Haftungsfragen, Gerichtsstand und anwendbares Recht auch hinsichtlich geltender Datenschutzbestimmungen.

Dokumentation

Dokumentationen in einer hybriden Infrastruktur sollten sich inhaltlich nicht von denen einer eigenen Rechenzentrumsinfrastruktur unterscheiden. Dokumente, Berichte und Prüfprotokolle müssen ebenso für beaufsichtigende Behörden, wie auch für Notfallkonzepte, zur Verfügung stehen.

Natürlich gibt es Unterschiede bzgl. der Assets, die in eine Dokumentation einfließen. Meist sind die genauen Assets gar nicht bekannt und müssen dies auch nicht sein, da hier der Service im Vordergrund steht und deren Bereitstellung. Bei Dokumentationen von hybriden Umgebungen sollte somit die Service-Ansicht im Vordergrund stehen, bzw. wo und wie dieser bereitgestellt wird.

Meldezuständigkeiten und Auditierung

Die Meldezuständigkeiten sind sehr klar geregelt, im Bereich Finanzdienstleistungen zum Beispiel durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), sowie die EBA (European Banking Authority) bzw. die Bankenaufsicht der Europäischen Zentralbank.

Außerhalb der Finanzindustrie bezieht sich das Thema Meldezuständigkeit hauptsächlich auf die Anbieter von Cloud-Diensten, die hier entsprechende Nachweise den Behörden vorlegen müssen.

Eine weitere Dimension sind die Betreiber kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes. Diese müssen eine Kontaktstelle benennen, IT-Störungen melden, den »Stand der Technik« umsetzen und dies alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen.

Regularien

In Deutschland sehr verbreitetet ist der IT-Grundschutz des BSI, in dem diverse Aspekte der Informationssicherheit abgebildet werden. In der aktuellen Version sind zehn unterschiedliche Bausteine von »Sicherheitsmanagement« über »Betrieb« bis zu »Netze und Kommunikation« abgedeckt.

Im BSI Cloud Computing Compliance Criteria Catalogue, kurz BSI C5, sind die Mindestanforderungen an die Informationssicherheit für Cloud-Dienste beschrieben. Dort sind in der Version 2020 auch die Anforderungen des EU Cybersecurity Acts (EUCA) aufgenommen. Testierungen nach BSI C5 erfolgen durch einen Wirtschaftsprüfer und werden im Ergebnis auch von diesem verantwortet. Im Bereich der Bankenindustrie existieren über IT-Grundschutz und BSI C5 überlagerte Regularien, die von der BaFin bzw. EBA herausgeben sind. Diese folgen dem Proportionalitätsprinzip und werden im Rahmen von Sonder- bzw. IT-Prüfungen durch die BaFin/Bundesbank und die EZB individuell bei den Instituten überprüft.

Ausstiegstrategien

Wie oben beschrieben, ist beim Nutzen von Hybriden Cloud-Modellen bereits beim Einrichten darauf zu achten, wie ein eventueller Umstieg oder Ausstieg durchgeführt werden kann. Ein entscheidender Punkt hierbei ist, darauf zu achten, dass die vom Anbieter erbrachten Leistungen bis zum Ende der Vertragslaufzeit auch nutzbar sind. Hierbei ist auf die komplette Kommunikationskette zu achten. Sonst kann beispielsweise auf laufende virtuelle Systeme wegen fehlender Netzwerkkomponenten nicht mehr zugegriffen werden.

Im Vertrag sind Kündigungsrechte und Fristen zu vereinbaren, welche auch Sonderkündigungsrechte enthalten, falls die Leistungserbringung grob von den vereinbarten Leistungen abweicht.

Neben den vertraglichen Aspekten sollten im Idealfall bereits in der Planungsphase auch technologische und architekturelle Überlegungen zu möglichen Ausstiegsstrategien erfolgen. Während IaaS (Infrastructure as a Service) relativ generisch ist, bieten die verschiedenen Clouds weitere Services an. Diese bieten häufig eine gute Integration innerhalb der Plattform, hohen Nutzwert und geringe Aufwände bei der Implementierung, sind dagegen aber meist proprietär und können daher weder einfach portiert oder gar migriert werden. Für viele der Dienste kann man mit vertretbarem Aufwand bereits auf Microservices / Container-Technologien umstellen, da diese von allen Clouds unterstützt werden und somit eine deutlich einfachere Portierung ermöglichen.

Die so genannte »Data Gravity« ist ein weiterer wichtiger Aspekt in den Ausstiegsszenarien. Dabei geht es primär darum welche Dienste noch von den Daten abhängen und wie weit man diese davon trennen kann. Im schwierigsten Fall sind am Ende alle Dienste so ineinander verzahnt und voneinander abhängig, dass nur ein kompletter Wechsel der Plattform bzw. des Anbieters in Frage kommt. Für eine Migration hat die Datenmenge auch einen wesentlichen Einfluss. Ist man z.B. gezwungen auf Grund von Insolvenz, rechtlichen Aspekten oder anderen Gründen seine Daten innerhalb eines kurzem Zeitfensters zu migrieren, so müssen auch die technischen Gegebenheiten dies ermöglichen, was nicht immer gegeben ist. Daher nutzen manche Ihren eigenen Storage als primären und zentralen Datenspeicher und binden von zentralen Punkten aus ihren jeweiligen Clouds ein. Dies erhöht zwar geringfügig die Komplexität, kann aber Kosten sparen und den Wechsel auf Verarbeitungsebene vereinfachen. Sogar Disaster Recovery Use Cases zwischen mehreren Clouds sind damit möglich.

Mitarbeiterausbildung

Die Bereitstellung einer hybriden Infrastruktur bedingt, dass ein Arbeitgeber auch bei Auslagerung von einzelnen Diensten in die Aus- und Weiterbildung seiner Mitarbeiter weiterhin investieren muss. Gerade die Schnelllebigkeit von Cloudtechnologien macht ein kontinuierliches Lernen unabdingbar. Wird hier regelmäßig investiert, können die Mitarbeiter den bereitgestellten Dienst besser bewerten und im Falle eines Ausstiegs aus dem Vertragsverhältnis auch den möglichen Umzug fachgerecht begleiten, oder die Arbeit eines eventuell hinzugezogenen Dienstleisters besser beurteilen. Sich im Rahmen eines Ausstiegs erst um ausgebildete Mitarbeiter durch Neueinstellung zu kümmern, kann aufgrund des Fachkräftemangels ein Problem darstellen.

Sollten Teile einer hybriden Infrastruktur verlagert oder nicht mehr benötigt werden, stehen meist die Daten im Fokus. Wie können diese verlagert werden, bzw. müssen sie überhaupt verlagert oder können sie neu erzeugt werden (z.B. Backupdaten)? Meist ist der Abzug von Daten aus einer Infrastruktur, die von Providern bereitgestellt wird, deutlich schwieriger (Zeit) als das »Betanken« einer solchen Infrastruktur. Ausstiegsabhängigkeiten wie Datenlöschung, Bereitstellung oder Dokumentationen sollten daher schon zu Beginn der Vertragsgestaltung aufgenommen werden.

Besonderheit der Governance in einer Hybriden IT

Governance-Aspekte, wie sie in diesem Kapiteln beschrieben wurden, haben einen deutlich höheren Fokus als in einer klassischen »inhouse« Umgebung. Gerade die Themen Auditierbarkeit, Dokumentation und Datensicherheit müssen bereits sehr früh in der Planung und Vertragsgestaltung berücksichtigt werden.

Quellen

Rundschreiben 09/2017 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk
Bankaufsichtliche Anforderungen an die IT (BAIT)
Die EBA Leitlinien zu Auslagerungen
Die EBA Guidelines on Information and Communication Technology and security risk management
↗**https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutz-About_node.html**
↗**https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog_node.html**

Weitere Quellen

Merkblatt – Orientierungshilfe zu Auslagerung an Cloud-Anbieter (BaFin)
Empfehlungen zur Auslagerung an Cloud-Anbieter (EBA – European Banking Authority)

6 Commercial

6 Commercial

Hybride IT bedeutet für Unternehmen zumeist, dass Teile der vom internen Kunden bezogenen IT-Services von der hausinternen IT-Abteilung selbst erbracht (»Make«), andere von einem oder mehreren Dritten bezogen werden (»Buy«). Grundsätzlich ist zu beachten, dass für diese verschiedenen Bezugswege auch verschiedene kommerzielle Rahmenbedingungen gelten.

Stark vereinfacht besteht der kommerzielle Teil der »Make«-Seite darin, Hardware (ggf. mit Wartungsverträgen) einzukaufen, diese mit eigenem Personal zu betreiben und die hierfür notwendigen Facility-Services wie Räumlichkeiten oder Stromversorgung von den entsprechenden internen Abteilungen zu beziehen. Entsprechend sind auch die Auswahl- und Vergabeverfahren, Freigaberegelungen und Budgetplanungen auf diese weitgehend interne Leistungserbringung und die mehrjährigen Beschaffungszyklen ausgerichtet.

Im Gegensatz hierzu erfolgt – wiederum stark vereinfacht skizziert – der Bezug von Dienstleistungen Dritter (»Buy«) recht dynamisch: Die von verschiedenen Managed-Service-Providern oder Public Clouds angebotenen Services sind zum einen schwer untereinander vergleichbar, zum anderen unterliegen sie recht kurzen Produktzyklen. Zudem werden sie meist im »pay-per-use«-Modell, also der tatsächlichen Nutzung entsprechend, abgerechnet. Für die Auswahl solcher Services müssen daher auch neue kommerzielle Bewertungskriterien gefunden werden.

Diese Dynamik und die nutzungsbasierte Abrechnung haben starke Auswirkungen auf den Budgetierungs-, Bezugs-, Freigabe- und Controlling-Prozess:

- Der bisherige, Hardware-basierte Bezug von IT-Services macht es schwer, den wirklichen Bedarf an Services wie virtuellen Maschinen und Laufzeit abzuschätzen, zumal der Betrieb bestehender Applikationen selten auf dynamisches, auf die wirkliche Last reagierendes Up- und Downsizing ausgelegt sind. Dies stellt eine Herausforderung für die Bedarfsabschätzung dar.

- Die Abrechnungsmodelle für Services, gerade diejenigen von Public-Cloud-Providern, führen neue Kostenbestandteile ein, wie beispielsweise den ausgehenden (»egress«) Datenverkehr. Dies stellt eine zusätzliche Herausforderung für die Budgetierung dar.

- Sollen Services vom Cloud- oder Service-Provider bezogen werden, liegt deren Stärke darin, dynamisch auf Bedarfsschwankungen zu reagieren. Diese kurzfristigen Änderungsmöglichkeiten können aber nur ausgeschöpft werden, wenn kundenseitig Bezugs- und Freigabe-Prozesse angepasst werden, um beispielsweise Bestellungen über die Providerportale ermöglichen. Dies stellt eine Herausforderung für die traditionelle Gewaltenteilung im Einkauf (doppelte Unterschrift bzw. 4-Augen-Prinzip) und die Abbildung in den bestehenden Compliance-Richtlinien dar.

- Generell unterliegen Service-Verträge anderen juristischen Rahmenbedingungen als der klassische Kauf- oder Leasingvertrag. Zu den juristischen Unterschieden in der Zusammenarbeit mit Managed-Service-Providern kommt hinzu, dass sich Kunden darauf einstellen müssen, den Public-Cloud-Provider-eigenen Vorgaben folgen zu müssen. Diese sind deshalb kaum nachzuverhandeln, damit diese ihre weltweiten Standards und Service-Level gewährleisten können. Zudem stellen sich Fragen zum Ort der Leistungserbringung und damit auch des

geltenden Rechtsraums. Dies stellt eine Abweichung zu den bislang zugrunde gelegten, eigenen Einkaufs-AGBs dar.

- Ist ein nutzungsbasiert abgerechneter Service erst einmal in Betrieb, stellt sich bald die Frage nach der Zuständigkeit und Verantwortlichkeit für die Kostenoptimierung – möglicherweise erweitert sich hierdurch der Zuständigkeitsbereich für die auf das Verbrauchsmodell zu sensibilisierenden IT-Administratoren. Dies stellt bedeutet eine Anforderung für Rollenbeschreibungen und Schulungsbedarf in der IT-Abteilung.

- Dynamische Kostenverläufe, wie sie die Ausnutzung eines pay-per-use-Abrechnungsmodells bewirken können, erfordern anstelle traditioneller Controlling-Ansätze ein Live-Monitoring der Kosten, beispielsweise innerhalb eines Provider-Management-Teams, um Überraschungen bei der nächsten Monatsabrechnung zu vermeiden. Hieraus ergibt sich eine Anforderung für Rollenbeschreibungen und Schulungsbedarf in der Finanzabteilung.

Durch all diese Herausforderungen ist die kommerzielle Seite beim Auslagern von Services an Dritte nicht zu unterschätzen. Zu beachten ist weiterhin, dass beim Betrieb hybrider IT die bisherigen Aufgaben, Zuständigkeiten und Verantwortlichkeiten nicht wegfallen, sondern zusätzliche neue hinzukommen. Schließlich werden »Make«- und »Buy«-Modelle parallel angewendet.

Zu beachten ist außerdem, dass auch beim Betrieb Hybrider IT-Redundanzen wie beim traditionellen IT-Aufbau sichergestellt werden müssen. Trotz vertraglich vereinbarter Service-SLA kann es auch beim Provider zu Service-Einschränkungen kommen, und die für einen solchen Fall vereinbarten Pönalen für Minderleistung decken in den seltensten Fällen den Schaden des Anwenderunternehmens ab.

Trotz aller Herausforderungen bei der erstmaligen Implementierung hybrider IT können sich jedoch auch große kommerzielle Vorteile ergeben, wenn die folgenden Rahmenbedingungen beachtet werden:

- Idealerweise werden vor allem bereits standardisierte oder leicht zu standardisierende Services zum Service-Provider oder in die Public Cloud ausgelagert, um kommerzielle Vorteile zu erwirken.

- Das Betriebs- und Preismodell des Service- oder Cloud-Providers muss zum Nutzungsverhalten des Kunden passen, die Migration der »falschen« Workloads kann leicht zu Kostensteigerungen anstelle der erhofften Einsparungen führen.

- Neben der technischen ist auch die kommerzielle Dimension vielschichtig. Prozessoptimierungen, Leistungszugewinne mit kommerziellen Vorteilen an anderer Stelle oder generelle Vereinfachungen mögen erhöhte Fremdkosten für den einzelnen Service aufwiegen.

- Hybride Modelle eröffnen die Möglichkeit, nach technischer und kommerzieller Validierung geeignete Teilbereiche auszulagern – und andere Teile traditionell fortzuführen.

7 Change

7 Change

Systeme, Prozesse oder Organisationen ändern sich fortwährend in der IT, weshalb viele Unternehmen dem Change-Prozess selbst keine große Aufmerksamkeit schenken. Bedenkt man jedoch den Aufwand für die Änderungen selbst sowie die immer wieder zu durchlaufende Lernkurve für neue Systeme und Prozesse, so wird schnell klar, dass nur ein professionelles Change-Management die Produktivität hoch und die assoziierten Kosten unter Kontrolle halten kann.

Organisational Change-Management dient zur strukturierten Vorbereitung, Durchführung und Nachbereitung von größeren Änderungen in Unternehmen. Mitarbeiter müssen verstehen, was der Sinn einer Änderung ist, was sich für Sie ändert und was ihre Rolle in der neuen Umgebung bzw. im neuen Prozess sein wird.

Menschen scheuen Veränderungen, da diese immer Unsicherheit und den Verlust von gewohntem und eingeübtem Wissen mit sich bringt. Daher ist es wichtig, die Änderungen im Vorfeld zu erklären, Sinn und Zweck klar darzustellen und jeden Einzelnen, der von der Änderung betroffen ist, auch adäquat abzuholen und mitzunehmen. Change-Manager arbeiten daher sowohl mit der Fachabteilung als auch der IT sowie der Personalabteilung zusammen, um den Mitarbeitern die Informationen und Schulungen an die Hand zu geben, damit sie den Change erfolgreich bewältigen können. Viele Unternehmen unterschätzen die positive Wirkung eines professionellen Change-Managements und erwarten von Mitarbeitern die spontane Akzeptanz einer neuen Software sowie die unmittelbare Perfektion in der Anwendung. Dass dies auf beiden Seiten zur Frustration führt, ist offensichtlich.

Ist bei der Planung und Umsetzung von hybriden IT-Modellen ein Teil der Tools, Prozesse und Plattformen neu, so greifen diese in bewährte und bekannte Arbeitsabläufe ein und verursachen bei den IT-Mannschaften ein Gefühl der Verunsicherung. Unternehmen, die ihre Teams in diesem Prozess aktiv unterstützen, Schulungen anbieten, Klarheiten schaffen über Nutzen und neue Rollen, profitieren von einer wesentlich schnelleren Adaption und einer besseren Lernkurve bei gleichzeitig geringerem Verlust an Produktivität. Change-Management bedarf Mittel und Ressourcen, die aber geringer ausfallen als der Rückgang an Produktivität, wenn der Change einfach passiv erwartet wird. Ebenso wird die Zeit bis zur vollständigen Adaption der neuen Umgebung kürzer ausfallen, wenn die Mitarbeiter den Sinn und Zweck des Neuen sowie die eigenen Mehrwerte besser verstehen.

8 Business Continuity

8 Business Continuity

Kritikalität von geschäftskritischen Prozessen und Applikationen – K-Fall Management

Wie im klassischen IT-Betrieb haben auch in der hybriden IT unterschiedliche Services verschiedene Auswirkungen auf den Geschäftsbetrieb. Deswegen gilt es im hybriden Betrieb, zuerst die Kritikalität des Service festzulegen, also zu definieren, welchen Einfluss die jeweilige Applikation bzw. Service auf das Unternehmen hat.

Dazu sollten auch die Abhängigkeiten zu anderen Services erfasst werden und welche RTO bzw. RPO notwendig ist. RTO beschreibt die maximale Ausfallzeit und RPO, wie viele Daten verloren werden können. Gemäß ITIL IT Service Continuity Management, sollte man die Priorisierung nach Eintrittswahrscheinlichkeit und Schadenshöhe anordnen.

In einem hybriden IT-Betrieb gibt es, im Vergleich zum klassischen und reinen On-Premises Betrieb, jedoch viele Unterschiede zu beachten.

So sind die SLAs bei den Public-Cloud-Services der Hyperscaler häufig anders definiert. Während z.B. im On-Premises Datacenter Storage in der Regel eine (gemessen erreichte) Verfügbarkeit von 99,9999% oder mehr aufweist (entspricht nur etwas mehr als 30 Sekunden Ausfallzeit pro System pro Jahr), wird dazu z.B. beim Hyperscaler eine Verfügbarkeit von 99,99 % für Block Volumes angestrebt (gemessen über beide Rechenzentren einer Region). Diese Verfügbarkeit teilt sich teilweise auch noch in weitere Komponenten auf, so wird bei Containern für die Control-Plane eine Verfügbarkeit von 99,95 % angestrebt (zählt, wenn alle Requests im 5-Minuten-Intervall fehlschlagen), für die Nodes hingegen 99,99 %.

Wie im Beispiel erwähnt, zählen die Werte in der Public Cloud nur, wenn beide Rechenzentren einer Region genutzt werden. Dies hat eine essenzielle Bedeutung für fast alle Use-Cases im Public-Cloud-Umfeld, grundsätzlich sollten nämlich mehrere Rechenzentren und häufig auch mehrere Regionen genutzt werden, um eine adäquate Verfügbarkeit bzw. Desaster-Fähigkeit zu erreichen.

Gibt es extrem hohe Anforderungen an die Verfügbarkeit, sollte man auch abwägen, eventuell mehr als eine Plattform zu verwenden, z.B. über einen Verbund aus On-Premises und Public-Cloud-Ressourcen oder auch mehr Cloud-Plattformen als nur diejenige von einem Hyperscaler. Obwohl die Aufwände gegen einen größeren Ausfall der Anbieter sehr hoch sind, kam es in der Vergangenheit dennoch (wenn auch selten) zu flächendeckenden Störungen.

Eine Kombination zwischen On-Premises und der Public-Cloud oder auch zwischen verschiedenen Hyperscalern bedarf grundsätzlich einer guten Planung, da z.B. eine virtuelle Maschine nicht einfach portierbar ist und zudem ein Abgleich der Daten zwischen diesen beiden erfolgen muss. Ebenso muss bei der Netzwerkarchitektur an einen nahtlosen Zugriff zwischen Frontend und Backend beim Wechseln der Umgebungen bedacht werden. Dies ist insbesondere bei Legacy-Applikationen meist schwieriger in der Umsetzung, als wenn man containerisierte

Anwendungen einsetzt. Ein Container-Image lässt sich sehr einfach in allen Umgebungen (Hyperscaler, -On-Premises oder beim Service Provider) starten und einsetzen. Zudem sind natürlich noch die Daten zu replizieren, die Verbindungen herzustellen und das Management dafür zu betreiben.

Die großen Cloud-Anbieter spielen Ihre Stärken insbesondere dann aus, wenn man deren native Cloud-Services verwendet. Dies bietet nicht nur den Vorteil, dass man beim Konsumieren der Services einen Teil der Betriebsaufgaben abgibt, sondern häufig auch einfach eine bessere Verfügbarkeit zu geringeren Kosten erreicht. Allerdings begibt man sich dabei oft in eine proprietäre Lösung, bei der man nicht mehr einfach interoperabel zwischen verschiedenen Anbietern oder On-Premises Daten replizieren kann. ISVs können eine Brücke zwischen verschiedenen Anbietern oder On-Premises bieten, da ihre Produkte oft in vielen Umgebungen laufen können und sie über ihre Mechanismen die Daten replizieren. Dies kann für Datenbanken, Storage und viele weitere Services bereits heute schon genutzt werden.

Wer heute mit »Frozen Zones« arbeitet, also Zeiträumen, in denen jegliche Changes, die nicht zur Störungsbeseitigung dienen, untersagt sind, sollte bei Konzepten mit externen Anbietern berücksichtigen, dass dies häufig nicht mehr eingefordert werden kann. Auch ein direkter Zugriff auf die Betriebsmannschaft des Providers gestaltet sich schwieriger.

9 Provider Management

9 Provider Management

Viele Unternehmen nutzen mehr als einen Anbieter (Service-Provider) um ihre Services zu beziehen. Da die verschiedenen Provider meist auch unterschiedliche Leistungen, Abrechnungsmodelle, Service Levels, Connectivity-, Vertrags- und Compliance-Modelle sowie Sicherheitsarchitekturen bieten, gestaltet sich das Management des Leistungsbezugs oft aufwendig.

Wichtig ist daher im Vorfeld eine klare Definition der Anforderungen zu erarbeiten und die Angebote auch während der Laufzeit regelmäßig auf die relevanten Parameter zu prüfen und das Management so weit wie möglich zu automatisieren. Kosteneinsparungen durch günstige Anbieter können z.B. durch aufwendige Verwaltung oder bei mangelnder Einhaltung von Compliance- oder Sicherheitsvorgaben schnell ins Gegenteil umschlagen.

Wie viele verschiedene Provider sinnvollerweise genutzt werden, hängt stark vom einzelnen Unternehmen und seinen IT-Services ab. Generell ist daher das Providermanagement als Funktion der Corporate IT als Funktion sinnvoll, da sich die Anbieterlandschaft über die Zeit immer wieder ändert. Providermanagement kümmert sich um die Aufstellung der Anforderungen sowie um die Audits der Service-Provider und stellt die erforderlichen Tools und Prozesse zur Verfügung.

Speziell bei Hybriden IT-Umgebungen ist durch die unterschiedlichen Arten der Leistungen ein Providermanagement unerlässlich, da ansonsten die übergreifende Integration, das Kosten- und Vertragsmanagement sowie die Optimierung des Portfolios nicht sinnvoll möglich sind.

10 Maintenance

10 Maintenance

Mit Maintenance ist die allgemeine Wartung der Gesamtlösung eines Service zu betrachten. Man unterscheidet dabei folgende Typen:

Hardware-Wartung

Hier steht die Pflege der Hardware-Komponenten im Fokus – dies beinhaltet den Austausch defekter oder veralteter Komponenten sowie das Update von Firmware- und Bios-Versionen. Dies betrifft sowohl das Netzwerk, Compute, Storage als auch Infrastruktur-Komponenten wie Klimatechnik und die Unterbrechungsfreie Stromversorgung (USV).

Software-Wartung

Die Software-Wartung umfasst die Pflege der genutzten Softwarekomponenten. In der Regel wird damit das Einspielen von Software-Updates und -Upgrades verbunden. Sie stellen Fixes für Sicherheitslücken, Fehlfunktionen oder Funktionserweiterungen bereit. Diese Wartung kann von einem externen Dienstleister (bspw. dem Hersteller bzw. Distributor) oder durch eigene IT-Abteilungen erbracht werden.

In dieser Betrachtung wird der Fokus auf die Software-Wartung gesetzt – die Wartung der Hardware (Firmware- und Bios-Updates, Hardware-Austausch) bleibt in der Verantwortung der einzelnen Plattform und wird als gegeben betrachtet.

In einer hybrid betriebenen IT werden unterschiedliche Plattformen miteinander kombiniert – die Wartung jeder einzelnen Plattform hat direkte Auswirkungen auf die Verfügbarkeit des gesamten Services und muss somit bereits bei der Planung der Architektur mit einbezogen werden.

In der klassischen IT-Welt werden oft fest definierte Wartungsfenster genutzt, in denen Servicearbeiten durchgeführt werden. Eine Unterbrechung der Verfügbarkeit ist möglich (Service Downtime), kann aber durch die Nutzung von redundanten Ressourcen (z.B. Clustering) vermieden werden. Jede Veränderung des Systems birgt Risiken – die mit entsprechenden Test- und Staging-Methoden reduziert werden können. Allerdings bleibt immer ein Restrisiko und daher wird die Wartung immer in geringen Lastzeiten durchgeführt. Wartungsfenster können bei der Nutzung von externen Plattformen nicht immer frei geplant werden – der Betreiber der Infrastruktur gibt hier seinem SLA folgend einen Rahmen vor.

Moderne Anwendungen, die dem DevOps-Konzept folgen, haben sehr kurze Lebenszyklen und somit andere Anforderungen an die Wartungskonzepte. Updates werden nicht mehr in gesonderten Wartungsfenstern eingespielt, sondern sind Bestandteil des normalen Betriebs und spiegeln sich in Konzepten von Continuous Integration und Continuous Deployment/Delivery wider.

In einer hybriden Umgebung können unterschiedliche Plattformen und unterschiedliche Software-Technologien kombiniert werden, die Wartung ist somit in zwei unterschiedlichen Dimensionen (Plattformkonzept ↔ Softwarekonzept) zu betrachten.

Des Weiteren ist zu betrachten, durch wen die Wartung erbracht wird – bei der Einbeziehung von SaaS-Diensten wird die Wartung dieser Dienste aus der eigenen Hand an einen externen Dienstleister abgegeben. Dies kann Kosten reduzieren, muss aber bei der Planung des Wartungskonzeptes mit betrachtet werden und erhöht gleichzeitig die Komplexität.

11 Migration

11 Migration

Eine Migration in die Cloud ist immer projektabhängig; hier gilt es, ein gemeinsames Verständnis zu definieren, was im Detail migriert bzw. auf welcher Ebene betrachtet werden soll. Eine Migration geht mit der Verlagerung von bestehenden Diensten, Plattformen oder Software-Versionen (Upgrades) einher. Im Gegensatz zur Migration kann eine Erweiterung der eigenen IT-Landschaft durch externe Dienste eine Inbetriebnahme bedeuten. Das Portfolio wird dadurch ergänzt, bestehende Systeme nur rudimentär verändert, aber nicht migriert. Migrationen sind i.d.R. komplex und müssen entsprechend geplant werden. Oft geht eine Migration mit dem parallelen Aufbau neuer Plattformen und der Einführung neuer Software einher. Daher ist eine einfache eins-zu-eins-Migration von Systemen i.d.R. nicht ausreichend, sondern es ist auch fast immer eine Migration von Daten erforderlich.

Bei Migrationen in hybriden Umgebungen ist darüber hinaus, aufgrund der Schnittstellen zwischen den selbst erbrachten und den gekauften Leistungen, eine klare Definition der gelieferten und zu erbringenden Leistung notwendig. Da die gekauften Dienste oft standardisiert sind, kann hier der Provider i.d.R. seine Leistung klar definieren. In konkreten Migrationsprojekten besteht die Herausforderung darin, die durch den Kunden zu migrierenden Dienste (Systeme oder Software) zu erfassen, und auf die vom Provider erbrachte Leistung abzubilden. Die häufig genannten Herausforderungen sind:

- Es existiert kein vollständiges Bild der bestehenden Infrastruktur.
- Durch Komplexität sind Abhängigkeiten der System- und/oder Anwendungslandschaft nicht transparent.
- Fehlendes Knowhow zur Erstellung einer Zielarchitektur der zu migrierenden Dienste,
- dadurch auch Unklarheiten über mögliche Betriebskosten auf der Cloud Seite.

Diese Themen muss der Kunde im Vorfeld klären. Oft kann ein Partner oder der Provider direkt seine Projekterfahrung und Best Practices einbringen, was auch für einen realistischen Zeitplan wichtig ist. Wichtig ist auch die enge Kommunikation über alle Bereiche hinweg. Das betrifft zum einen die direkt von der Migration betroffenen Bereiche wie z.B. Infrastruktur oder Anwendungsbetrieb, aber auch Security, Risk-Management und Compliance. Ein großer Schwerpunkt hier liegt in der Abbildung der ITIL-Prozesse um Incident-, Problem- und Change-Management, die in der Hybriden IT auch mit denen des Providers verknüpft sind.

Ein Cloud Migrationsprojekt besteht aus mehreren Phasen:

- Assessment
- Plan
- Prove
- Transform
- Test
- Go Live
- Rollback (optional)

Die wichtigsten Schritte sind Assessment und Planung. Hierbei ist es empfehlenswert, ein Tool-basierendes Assessment zwecks Analyse der Lastprofile einzusetzen, um z.B. Abhängigkeiten im Netzwerkverkehr transparent zu machen. Erst wenn die genauen Abhängigkeiten bekannt sind, kann abgeleitet werden, ob eventuell ganze VM- oder Anwendungsgruppen als Ganzes betrachtet bzw. migriert werden müssen. Eine genaue und realistische Abbildung der Server und Ressourcen auf Seiten der Cloud ist notwendig, um eine kostenoptimierte Zielumgebung zu schaffen. Bei Daten, die in die Cloud kopiert werden müssen, ist vorher genau zu prüfen, ob dies erlaubt bzw. Compliance-konform ist.

Das Design der Zielumgebung auf der Cloud Seite muss genau nach den Anforderungen geplant werden. Hierbei gibt es Rollenmodelle, Zugriffrechte, Abbildung von Groups/Abteilungen zu beachten. Netzwerkkommunikation, Netzwerkkonfiguration u.v.m. ist in einem Feinkonzept festzulegen. Eine erforderliche Änderung im Nachhinein kann unter Umständen sehr aufwendig bis hin zu unmöglich sein. Dies ist auch eine Voraussetzung, um ggf. versteckte Kosten ausfindig zu machen. Nur ein klarer Überblick ermöglicht es, zielgerecht zu planen und potenzielle Projektrisiken zu erkennen, bevor diese auftreten und kostspielige Nacharbeiten, sowie Qualitätsverluste der Zielumgebung bedeuten.

Ein weiterer wichtiger Punkt ist die Ermittlung der zu erwartenden monatlichen Kosten unter Einbeziehung von Optimierungspotenzialen wie Resizing, Snoozing oder bestimmte Abo-Angebote der Cloud Providern. Bei der Migrationsdurchführung kommen sehr oft Tools zum Einsatz. Hier bieten die jeweiligen Cloud-Provider-Plattformen bestimmte Tools zur Unterstützung an.

In der Testphase sollte auch ein Rollback mit eingeplant werden, also eine kurzfristige Rückumstellung, sofern bei der Inbetriebnahme unerwartete Probleme auftreten. Sofern eine Rückverlagerung in den Eigenbetrieb optional ist, ist aber auch die Möglichkeit für einen mittel- bis langfristigen Rollback vorzusehen. Hier muss aber bedacht werden, dass nach längerer Zeit des Betriebs durch einen Provider die eigene IT-Mannschaft oft nicht mehr das notwendige Knowhow besitzt, diese Landschaft On-Premises zu betreiben. Ein einfaches Zurück ist dann nicht mehr möglich und eine entsprechend aufwändige Migration wäre erneut erforderlich.

12 Monitoring

12 Monitoring

»Monitoring« im Bereich der IT handelt – allgemein gesehen – von der laufenden Überwachung der IT-Systeme auf ihre korrekte Funktionalität. Prozesse und IT-Vorgänge werden dabei in der klassischen IT überwacht und protokolliert. Der Ursprung des Monitorings lag in der Überwachung von:

- Compute
- Storage
- Network

Mit wachsenden Anforderungen wurde Monitoring immer weiter ausgedehnt. Die heutigen Standards umfassen außerdem:

- Application Monitoring
- End to end Monitoring
- SLA Monitoring (SLA = Service Level Agreement)
- Monitoring von Performance and Growth
- Disaster Recovery and Business Continuity

Neben diesen klassischen schon lange vorhandenen Monitoring-Lösungen kommen jetzt neue Monitoring-Anforderungen durch die Hybride IT auf die Verantwortlichen zu:

Die weltweite Akzeptanz von Containern nimmt drastisch zu, da eine stetig wachsende Anzahl von Firmen neue Anwendungen entwickelt und einsetzt. Gartner prognostiziert, dass 75 % aller Organisationen bis 2022 Container-Anwendungen eingeführt haben werden. Dies ermöglicht es der Anwendung, sehr flexibel Ressourcen entweder On-Premises oder as-a-Service zu nutzen.

Während das »Lift and Shift« traditioneller virtueller Maschinen (VMs) in Container üblich ist, kann das volle Potenzial und die Vorteile von Containern erst dann genutzt werden, wenn neue Cloud-native-Anwendungen unter Verwendung von Containern und Microservices entwickelt werden. Die Konvertierung ineffizienter VMs in Container sollte eigentlich eine temporäre Maßnahme sein und ist keine eigentliche Cloud- oder Container-Migrationsstrategie.

In diesem Szenario kommen spezifische Anforderungen der Hybriden IT- in Bezug auf die Überwachung hinzu. Diese betreffen vor allem die persistente Speicherung, das Datenmanagement, die Sicherheit und Multi-Cloud- oder Datenzentrum-übergreifende Unterstützung, anwendungsgesteuerte Überwachung (Prometheus), Kostenüberwachung (fachabteilungsgerecht). Die Container-Technologie ist der treibende Faktor beim für Hybride IT spezifischen Monitoring.

Traditionelles Monitoring setzt oft auf die Verwendung von Agenten auf. Der Agent überwacht die entsprechende Ressource und schickt seine Daten an die Monitoring-Instanz. Die Hardware-Ressourcen einer Cloud lassen sich so nicht überwachen – allenfalls ist es möglich, im Rahmen von »Lift and Shift« auch einen Agenten in der VM in die Überwachung zu integrieren.

Service-Provider stellen aber eigene Methoden zur Leistungsmessung bereit, diese können dann in das eigene Monitoring übertragen werden. Somit wird das Monitoring der Infrastruktur »agentless« betrieben. Wie im Bereich anwendungsbasiertes Monitoring beschrieben, kann dies dann auch auf die Anwendungsschicht erweitert werden.

Persistent Storage

Beim persistenten Storage handelt es sich um die fest zugeordneten Speicherbereiche, die einer VM, einem Container oder auch Applikation spezifisch zugeordnet sind. Die bekannten Messattribute wie Verfügbarkeit, Kapazität, Auslastung und Performance gelten auch hier. Neu ist die Agilität der Applikation und damit auch das häufige Verschieben von persistentem Storage. Das muss in einem Monitoring-System berücksichtigt werden.

Multi Cloud Support oder Cross Datacenter Support

In der Hybriden IT kann es durchaus vorkommen, dass die Applikationsteile eines Lösungs-Stacks verteilt betrieben werden. So kann eine Datenbank beispielsweise im eigenen Rechenzentrum, also On-Premises laufen. Ein erster Applikationsteil läuft bei einem Cloudanbieter und ein zweiter Teil bei einem zweiten Cloudanbieter. Auch Technologien wie »bursting« (also der temporären Zuhilfenahme von Cloud-Ressourcen zur Absicherung von Lastspitzen) gilt es in das Monitoring mit aufzunehmen. Hier muss das Monitoring aufzeichnen, wo und wann die verschiedenen Applikationsteile laufen. Das Monitoring muss dabei der Applikation automatisch folgen.

Anwendungsbasiertes Monitoring

In der traditionellen IT-Welt dominiert das Monitoring der Ressourcen (CPU/Speicher/Netzwerk). Container-basierte Umgebungen lassen sich dort nur bedingt integrieren, da die Agilität und fehlende Hoheit über die Infrastruktur nicht mit einer statischen Monitoring-Lösung zu erfassen ist. Hier zeigt sich allerdings auch der Trend, dass Anwendungen selbst geeignete Monitoring-Schnittstellen per API bereitstellen, die dann ein direktes Monitoring erlauben (Beispiel Prometheus als Open-Source-Projekt). In einer hybriden Umgebung ist zu beachten, dass für das Monitoring alle Komponenten (lokale wie dezentrale) integriert werden müssen, um somit einen gesamtheitlichen Blick auf den Zustand zu ermöglichen. Existierende Monitoring-Lösungen sollten beim Einsatz einer hybriden Infrastruktur entsprechend erweitert oder komplett überarbeitet werden.

Security

Durch das häufigere Verschieben zwischen On-Premises und as-a-Service-Bereichen gilt es, ein Security Framework aufzubauen, das die Sicherheitsanforderungen der genutzten Bereiche definiert. Das Monitoring Tool sollte (soweit als möglich) automatisiert diesen Rahmen auf Einhaltung prüfen. Die neu entstehenden Container-Applikationen müssen ebenfalls den Security-Richtlinien der DevOps- (DevSecOps-) Entwicklung gerecht werden und diesen folgen. Siehe hierzu auch den obenstehenden Abschnitt »Anwendungsbasiertes Monitoring«.

Erweiterte Monitoring-Parameter

Cloud-basierte Lösungen ermöglichen in der kommerziellen Betrachtung einen Wechsel von Investitionskosten zu Betriebskosten (CAPEX → OPEX). Bei ein einem »Pay as you use«-Modell sind die Kosten aber von der genutzten Leistung abhängig und müssen daher auch in ein Monitoring mit einbezogen werden.

Service-Provider bieten hierfür eigene Schnittstellen und Services an. Bei dem Einsatz einer Hybriden Lösung müssen daher die Kosten der lokalen (On-Premises) und der Remote-Anteile kombiniert werden. Dies ist sicherlich keine Kernaufgabe des Monitorings – es dient allerdings als Datenquelle und sollte daher in die Konzeption der Gesamtlösung mit einbezogen werden, um eine servicebasierte Verrechnung intern wie extern zu ermöglichen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom