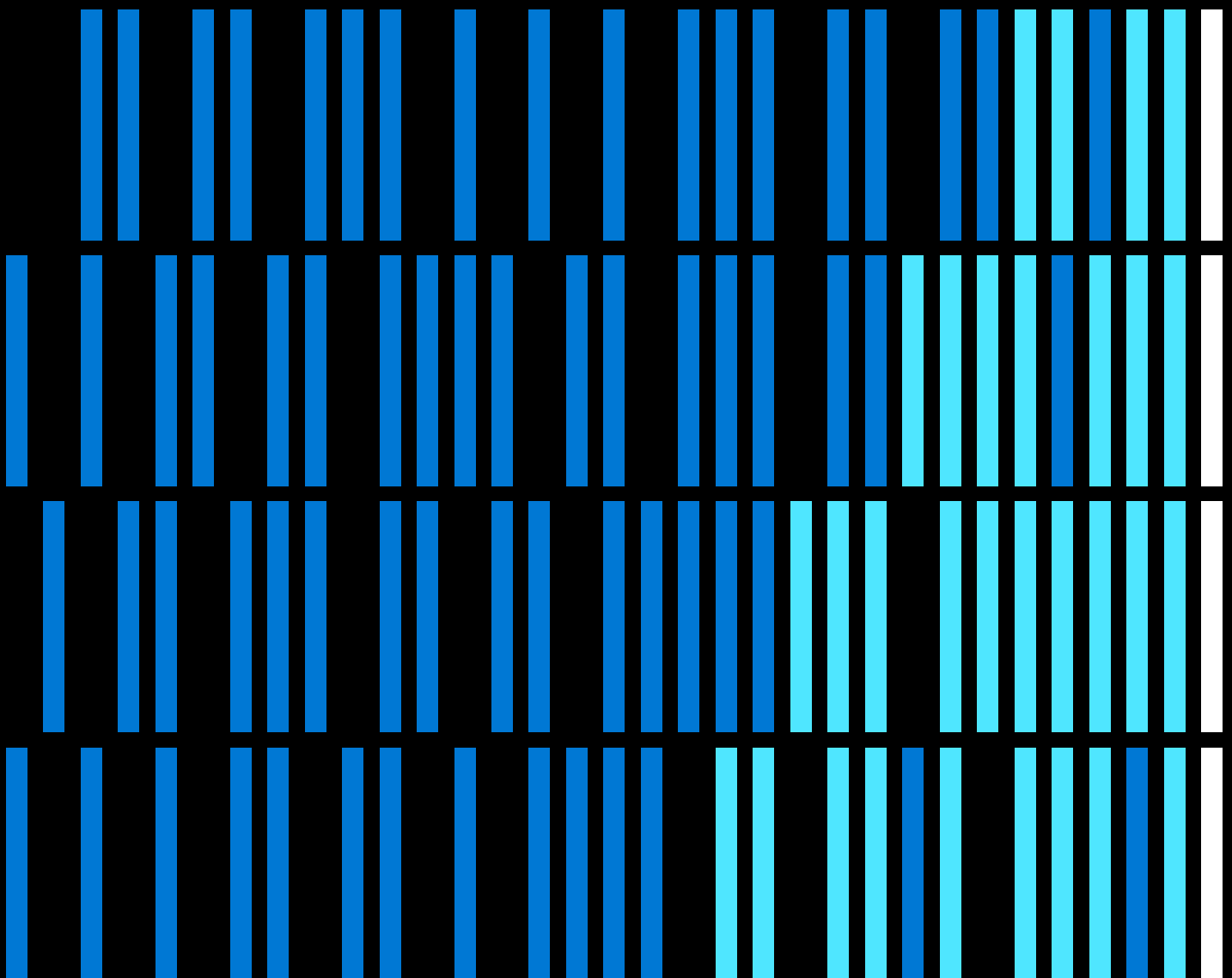


Enterprise Cloud Strategy

2. Auflage



VERÖFFENTLICHT VON
Microsoft Press
Ein Geschäftsbereich der Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2017 Microsoft Corporation

Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung darf kein Inhalt dieses Buchs in beliebiger Form oder auf beliebige Weise reproduziert oder übermittelt werden.

Bücher von Microsoft Press sind bei Buchhändlern und Distributoren weltweit erhältlich. Wenden Sie sich bei Fragen zu diesem Buch per E-Mail an Microsoft Press Support: mspinput@microsoft.com.
Teilen Sie uns Ihre Meinung zu diesem Buch mit: <http://aka.ms/tellpress>.

Dieses Buch wird „in der vorliegenden Form“ zur Verfügung gestellt und spiegelt die Ansichten und Meinungen des Autors wider. In diesem Buch dargelegte Ansichten, Meinungen und Informationen, einschließlich URLs und anderer Verweise auf Websites, können ohne vorherige Ankündigung geändert werden.

Einige Beispiele hierin sind fiktiv und dienen lediglich zur Veranschaulichung. Assoziationen oder Verbindungen mit tatsächlichen Beispielen sind nicht beabsichtigt und sind diesem Buch nicht zu entnehmen.

Microsoft und die auf der Website zu Marken unter <http://www.microsoft.com> aufgeführten Marken sind Marken der Microsoft-Unternehmensgruppe. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Acquisitions Editor: Janine Patrick

Developmental Editor: Bob Russell, Octal Publishing, Inc.

Redaktionelle Beiträge: Dianne Russell, Octal Publishing, Inc.

Copyeditor: Bob Russell

Das Festlegen der richtigen Cloud-Strategie für ein Unternehmen ist eine komplexe Aufgabe, die leicht zu verstehen, aber schwer zu meistern ist. Aus diesem Grund ist das E-Book *Enterprise Cloud Strategy* eine der besten Publikationen für Cloud-Experten, die erfahren möchten, wie Unternehmen den Umstieg auf die Cloud effizient bewerkstelligen können. Dieses Buch bietet eine verständliche und doch detaillierte Beschreibung aller Aspekte der Cloud-Strategie mit einer großen Sammlung von Fallstudien, wiederholbaren Mustern und sogar Cloud-Architektur-Blueprints, um die Umsetzung spezifischer Cloud-Anwendungsfälle zu beschleunigen. Es ist der perfekte Begleiter für alle Berater, Strategen und Unternehmensplaner, die komplexe Pläne für den Umstieg auf die Cloud erstellen – und Pflichtlektüre für all unsere Technologiestrategie-Experten. Es ist wichtig, dass das Buch technologiefremde Aspekte der Cloud-Strategie behandelt. Noch wichtiger ist jedoch, dass es dem Leser Leitprinzipien für die Implementierung von Cloud-Strategien an die Hand gibt. In erster Linie ist das Buch aber sehr angenehm zu lesen und in keiner Weise abschreckend für Neulinge im Bereich der Cloud.

– Miha Kralj, Managing Director of Cloud Strategy, Accenture

Der Umstieg auf die Cloud hat zahlreiche Möglichkeiten eröffnet. Zugleich erfordert er Best Practices und einen Leitfaden für die Einführung von Cloud-Plattformen mit der für Unternehmen notwendigen Exaktheit und Governance. Diese so dringend notwendigen Informationen werden im vorliegenden Buch in verständlicher, kurzer und praxisnaher Form bereitgestellt. Außerdem ist das Buch leicht zu lesen. Es basiert auf Best Practices von Microsoft IT und vielen globalen Unternehmen und stellt als solches einen Ansatz und Methoden vor, die ich Ihnen nur empfehlen kann. Ich wünsche Ihnen viel Glück auf Ihrem Weg zur Cloud.

– Gavriella Schuster, Corporate Vice President, One Commercial Partner,
Microsoft Corporation, Juli 2017

Das Buch *Enterprise Cloud Strategy* bietet einen strategischen und vor allem vollständigen Blickwinkel auf die Vielzahl von Problemen und Herausforderungen, vor denen Unternehmen im Zeitalter von Cloud Computing stehen und – was am wichtigsten ist – einen umfassenden Überblick über die Chancen, die die Cloud Unternehmen eröffnet. Von der strategischen Argumentation bis hin zu praktischen Tipps für die Beurteilung der Anforderungen und Prüfung bewährter Methoden – in diesem Buch erfahren Unternehmensarchitekten und Entscheidungsträger, worum es beim Cloud Computing geht und weshalb jedes moderne Unternehmen jetzt aktiv werden muss.

– Ulrich Homann, Architekt, Cloud und Enterprise Engineering, Microsoft

Inhalt

Einführung in die zweite Auflage	viii
Danksagungen.....	ix
Kostenlose E-Books von Microsoft Press.....	ix
Teil I: Die Anfänge.....	x
Kapitel 1: Die Cloud, Effizienz und Innovation	1
Enterprise-Computing vor der Einführung der Cloud	1
Wirtschaftlichkeit der Cloud.....	2
Nach den Gesamtbetriebskosten (TCO): Der Weg zur Cloud geht weiter	4
Innovation	5
AccuWeather.....	6
GEICO.....	6
Rolls-Royce	7
Brainshark.....	7
Katastrophenhilfe: Oso (Washington) 2014 und Nepal 2015.....	8
Erkenntnisse.....	9
Kapitel 2: Was ist die Cloud?.....	10
Public, Private und Hybrid Clouds	11
Private Cloud.....	11
Public Cloud	11
Hybrid Cloud.....	11
Skalierbarkeit macht Computing zu einem On-Demand-Service.....	12
„As a service“	12
Infrastructure as a Service.....	13
Platform as a Service (PaaS).....	13
Software as a Service (SaaS)	14
Container	14
„As-a-Service“-Modelle im Vergleich	15
Kapitel 3: Der Weg zur Cloud: Planung.....	16
Modernisierungsmöglichkeiten nutzen.....	16
Die fünf Pfeiler der Modernisierung	17
Die drei Phasen der Cloud-Migration	19

Experimentieren.....	19
Migration.....	20
Transformation.....	20
Kapitel 4: Experimentieren.....	21
Die erste Cloud-Anwendung von Microsoft IT.....	21
Schatten-IT und die Kultur des Experimentierens.....	23
Prinzipien einer Kultur des Experimentierens.....	23
Teil II: Umstellung der IT auf die Cloud.....	26
Kapitel 5: Entwicklung der Voraussetzungen.....	27
Festlegen von Strategien und Zielen.....	27
Organisatorische Aufgaben bei der Entwicklung der Strategie.....	31
Unternehmensarchitektur.....	31
Informationssicherheit und Risikomanagement.....	32
Datenklassifizierung.....	33
Unternehmensrisikomanagement.....	34
Finanzmanagement.....	34
Operatives Geschäft.....	35
Personal und die Entwicklung von Rollen.....	37
Entwicklung von Fähigkeiten.....	38
Anwendungsteams.....	40
Geschäftseinheiten.....	41
Kapitel 6: Portfolioanalyse.....	42
Entwicklung des Katalogs.....	42
Top-down-Portfolioanalyse.....	43
Bottom-up-Portfolioanalyse.....	45
Kapitel 7: Entwicklung und Ausführen des Plans.....	48
Beginnen Sie zunächst mit Entwicklungs- und Testbereichen.....	48
Der Cloud-Migrationsplan.....	49
Tools.....	51
Abonnementverwaltung.....	51
Die Erfahrung von Microsoft IT.....	53
Kapitel 8: DevOps macht Teams produktiver.....	55
Nutzung der Cloud für Entwicklung und Tests.....	55
Die DevOps-Revolution.....	57
Kontinuierliche Integration und Bereitstellung.....	57
Überwachung und Instrumentierung.....	58
Optimieren Sie Ihre Infrastruktur mit DevOps.....	59
Ein Themenwechsel.....	61
Kapitel 9: Sicherheit und Governance in der Cloud.....	62
Cloud-Sicherheit.....	62
Physische Sicherheit.....	62

Softwareupdates.....	63
Umfassende Verschlüsselung.....	63
Schlüsseltresor und Hardwaresicherheitsmodule	63
Antivirensoftware	64
Mehrstufige Authentifizierung.....	64
Lebenszyklus für die sichere Entwicklung	64
Überwachung von Sicherheitsverletzungen	64
Penetrationstests.....	65
Verständnis von Cloud-Sicherheitskontrollen	65
Governance, Compliance und Risiko	65
Sicherstellen der Einhaltung gesetzlicher Vorschriften.....	67
Data Governance.....	68
Financial Governance.....	69
Änderungsverwaltung	69
ITIL und die Cloud.....	70
Teil III: Ein neues IT-Zeitalter	72
Kapitel 10: In die Cloud und wieder zurück	73
Sicherung und Wiederherstellung.....	73
Lokalen Speicher in die Cloud erweitern	75
Business-Continuity und Notfallwiederherstellung	75
Integration.....	75
Netzwerk.....	76
Messaging: Service Bus.....	77
Serverlose Anwendungsintegration: Logic Apps.....	78
Erweitern von Verzeichnisdiensten in die Cloud	78
Cloud Computing in Ihrem Rechenzentrum.....	79
Verwaltung von Hybrid Clouds.....	80
Kapitel 11: Neue Anwendungs-modelle	81
Was bedeutet Transformation?	81
Platform-as-a-Service (PaaS)	83
Container und Orchestrierung.....	85
Microservices	86
Aktorenmodell.....	87
Resilienz in der Cloud	87
„Serverlose“ Anwendungen.....	89
Kapitel 12: Alles dreht sich um die Daten.....	93
Enterprise Data Management vor der Cloud	94
Strukturierte Datenverwaltung	94
Unstrukturierte Daten.....	95
Enterprise Data Management im Zeitalter der Cloud.....	95

Wichtige Speicherkonzepte	95
Relationale Daten in der Cloud	96
Die zunehmende Bedeutung von NoSQL-Datenbanken	97
Big Data und Bigger Data	98
Der Data Lake	99
Analyse-Dienste und Datenvisualisierung.....	99
Kapitel 13: Entwickeln Sie mit KI Ihr Unternehmen erfolgreich weiter	100
Was umfasst KI und Machine Learning?	100
Machine Learning: Grundlagen	101
Überwachtes Lernen im Vergleich zu unüberwachtem Lernen	102
Neuronale Netze	103
Machine Learning mithilfe von Hardware beschleunigen	103
Die Nutzung von künstlicher Intelligenz und Machine Learning	103
Bots und dialogorientierte Computer	104
Prädikative Analysen	104
Autonomie	104
Betrugsermittlung und andere Finanzanwendungen	104
Die Nutzung im Gesundheitswesen	105
Zusammenfassung	105
Zusammenfassung	106
Anhang A: Cloud-Architektur-Blueprints	109
Digitales Marketing	110
Einfache digitale Marketing-Website.....	110
Skalierbare Umbraco CMS-Web-App	111
Mobil	112
Aufgabenbasierte mobile App für Verbraucher	112
Benutzerdefinierte mobile App für Mitarbeiter	113
Soziale mobile und Web-App mit Authentifizierung	114
Backup und Archivierung	115
Entwicklung und Test.....	116
Entwicklung und Test für IaaS.....	116
Entwicklung und Test für PaaS	117
Entwicklung und Test für Microservices-Lösungen	118
Notfallwiederherstellung.....	119
Unternehmensweite Notfallwiederherstellung	119
SMB-Notfallwiederherstellung mit Site Recovery in Azure.....	120
SAP auf Azure	121

SAP HANA für Azure	121
SAP Hana auf Azure Architektur (große Instanz)	122
Hochleistungs-Computing	122
Big Compute-Lösungen als Service	122
In der Cloud bereitgestellte HPC-Cluster	123
On-Premises-HPC-Implementierung auf Azure laden	124
Digitale Medien	124
Digitale Medien: Video-on-Demand	124
Digitale Medien: Livestreaming	125
Schlagwortsuche/Spracherkennung/optische Bilderkennung bei digitalen Medien	126
E-Commerce	126
Internet der Dinge	128
Microservices-Anwendungen	129
Business Intelligence	129
Big Data und Analytics	129
Cloud-Migration	130
Data Warehouse	130
SaaS-Business-Apps	131
Spiele	131
Blockchain	132
Serie von Geschäftsanwendungen	132
DevOps	134
SharePoint auf Azure	134
Dynamics auf Azure	135
Hybrid Cloud-Szenarien	135
Hybrid Cloud-Konnektivität	135
Hybrid-Datenbankszenarien	137
Hohe Verfügbarkeit in der Cloud	138
Vernetzte Geräte	140
Identität und Authentifizierung	142
Enterprise Mobility-Verwaltung	143
Websites	144
Weiterführende Literatur	146
Azure-Ressourcen	146
Externe Websites	147
Bücher	147
Die Autoren	148

Einführung in die zweite Auflage

In den zwei Jahren seit dem Beginn unserer Arbeit an *Enterprise Cloud Strategy* hat sich viel verändert. Die Frage beim Thema Cloud-Technologie ist heute nicht mehr, ob die Cloud genutzt wird, sondern wann, und in fast allen Unternehmen ist die Cloud inzwischen ein fester Bestandteil der IT-Strategie. Darüber hinaus realisieren immer mehr Unternehmen, dass Cloud Computing nicht nur eine Reihe von technischen Möglichkeiten zur Effizienzsteigerung und Kosteneinsparung darstellt, sondern grundlegende Veränderungen im Bereich des Enterprise-Computings bewirken kann. In der Tat stellen viele Unternehmen fest, dass Cloud Computing gänzlich neue Geschäftsmodelle, Einnahmequellen und Möglichkeiten zum Stärken der Kundennähe bietet.

Einige technische Änderungen haben das Potenzial, die Art und Weise, wie wir Geschäfte machen, von Grund auf zu verändern. Die letzte derart fundamentale Veränderung erlebten wir bei der Einführung des Internets selbst.

Wie wir jedoch in der ersten Auflage dieses Buchs erwähnten, hören wir bei der Beratung von CIOs und IT-Führungskräften bei Microsoft häufig, dass die Migration der IT-Workloads zur Cloud zu den wichtigsten Prioritäten zählt. Und oft folgen auf diese Aussage Fragen wie „Womit fange ich an?“, „Wie entwickle ich einen Plan für die Cloudmigration meines gesamten Portfolios?“ und „Inwiefern wird meine Organisation von dieser Änderung betroffen sein?“.

Heute stellt sich eine weitere neue Frage: „Wie kann ich Cloud Computing auf wirklich gewinn- und nutzbringende Weise für das Unternehmen einsetzen?“

Dieses Buch, das auf den Erfahrungen von realen IT-Teams basiert, versucht, diese Fragen zu beantworten. Sie erfahren, was die Cloud so attraktiv für Unternehmen macht, welche Anwendungen Sie für Ihren Einstieg in die Cloud erwägen sollten, wie sich Ihre Organisation verändern wird, wie Kompetenzfelder weiterentwickelt werden, wie es um Sicherheit, Compliance und Buy-in bestellt ist und wie Sie die ständig wachsende Zahl von Funktionen der Cloud nutzen, um sich einen strategischen Vorsprung und Wettbewerbsvorteil zu verschaffen.

Danksagungen

Bei der zweiten Auflage möchten wir uns bei Miha Kralj, Managing Director of Cloud Strategy bei Accenture, und Brian Cawelti von Avanade bedanken, die uns ihre Einblicke zur Verfügung gestellt haben. Außerdem danken wir Brad Wright und Rick Ochs von Microsoft IT. Frank Simorjay, Ranger Due, Rodrigo Souza, David Cervigon Luna, Pete Apple, Andre de Beer, Brian Harrison und William Bories von Microsoft haben ebenfalls äußerst hilfreiche Beiträge geleistet.

Zudem danken wir den folgenden Personen für ihre Unterstützung, Beratung und Bereitstellung ihres Fachwissens: Scott Woodgate, Javier Nino, Tom Schinder, Venkat Gattamneni, Martin Vliem, Ulrich Homann, Robert Hanegraaff, John Devadoss, Brenda Carter, Michael Washam, Zoiner Tejeda, Nadia Matthews, Rob Beddard, Jeff Fryling, Kevin Gee, Colin Nurse, Raman Johar, Walter Myers, Uwe Hoffman, Ashish Sharma, Ashutosh Maheshware, Rich Nickerson, Michel Declercq, Arlindo Alves, Dennis Mulder, George Moore, Richard Ochs und Christopher Bennage.

Rob Boucher und Monica Rush haben die grafischen Darstellungen der Blueprints in Anhang A erstellt.

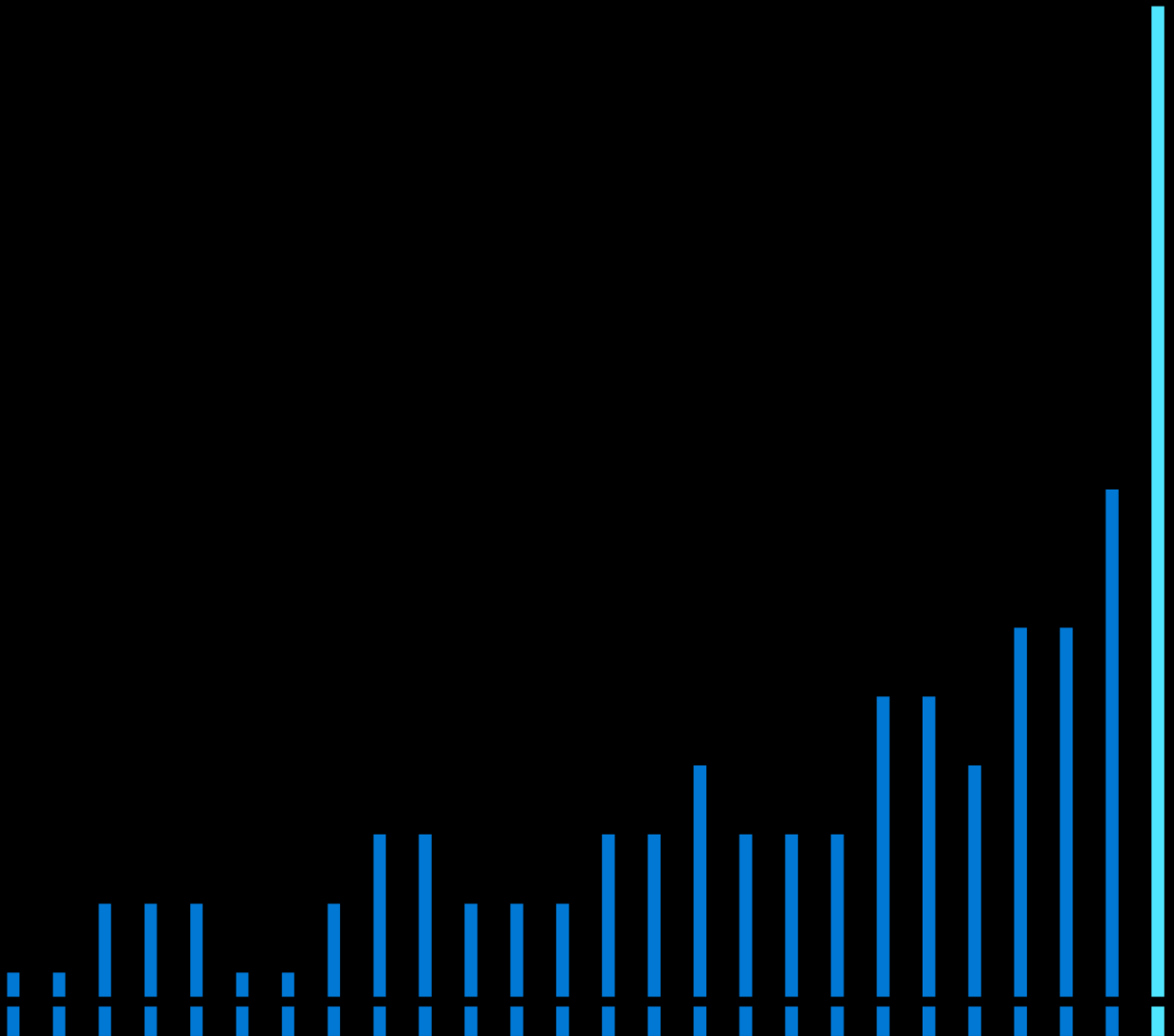
Kostenlose E-Books von Microsoft Press

Von technischen Übersichten bis zu detaillierten Informationen zu speziellen Themen – die kostenlosen E-Books von Microsoft Press decken eine große Auswahl an Themen ab. Diese E-Books sind als PDF, EPUB und Mobi for Kindle zum Download verfügbar: <http://aka.ms/mspressfree>

Die komplette Sammlung finden Sie unter <https://www.microsoftpressstore.com/>.

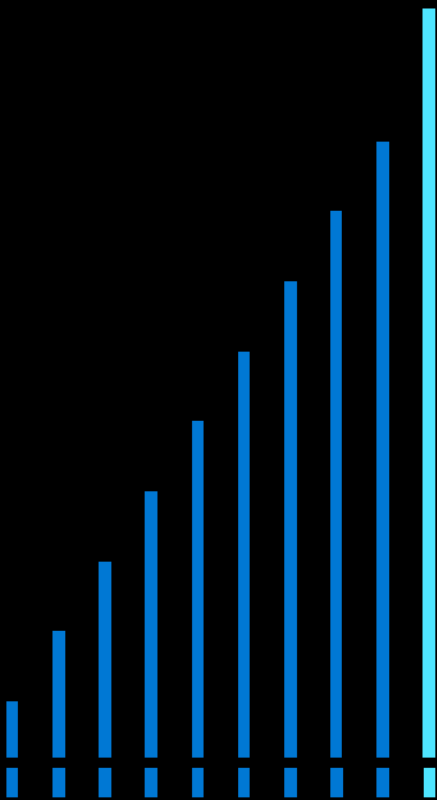
Teil I

Die Anfänge



Kapitel 1

Die Cloud, Effizienz
und Innovation



Die meisten Unternehmen bestätigen, dass die Cloud inzwischen ein zentrales Element ihrer Technologiestrategie darstellt. In den letzten Jahren haben wir erlebt, dass nicht mehr die Frage gestellt wird, ob die Cloud eingeführt wird, sondern wann und wie.

Nichtsdestoweniger stellt die Cloud eine der größten Veränderungen im Computerwesen dar. Daher lohnt es sich zu prüfen, warum sie so attraktiv für die Unternehmens-IT ist. Ihr Wertversprechen ist vielfältig und reicht von beträchtlichen Kosteneinsparungen im Vergleich zum Ansatz des traditionellen Rechenzentrums bis hin zur Möglichkeit der schnellen Entwicklung robuster Anwendungen, die bei steigendem oder abnehmendem Traffic herauf- bzw. herunterskaliert werden können.

Enterprise-Computing vor der Einführung der Cloud

Fast ein halbes Jahrhundert lang ist die Wirtschaftlichkeit von Enterprise-Computing relativ konstant geblieben. Unternehmen kauften Hard- und Software von Anbietern und betrieben sie in ihren eigenen Rechenzentren. Computer waren wie alle anderen Investitionen: eine (in der Regel große) einmalige Anschaffung, auf die mehrere Jahre der Abschreibung folgten.

Mit den Unternehmen wuchs aus verschiedenen Gründen auch die Anzahl von Rechenzentren. Beim Bau neuer Einrichtungen oder Betriebsanlagen wurde in der Nähe ein neues Rechenzentrum errichtet. Wenn Unternehmen in andere Länder expandierten, musste aus technischen Gründen (zur Verringerung der Nettwerkkosten) und vielleicht auch aufgrund der lokalen Bestimmungen ein Rechenzentrum an diesem Standort eingerichtet werden. Und als Computer für den Betrieb des Unternehmens geschäftskritisch wurden, wurden neue Rechenzentren gebaut – einzig und allein, um die Anforderungen hinsichtlich Business-Continuity und Disaster Recovery zu unterstützen.

Für den CIO war die Folge dieser Expansion eine IT-Organisation, die sich in manchen Fällen über den gesamten Globus erstreckte und viele qualifizierte Mitarbeiter zur Wartung all der Systeme erforderte. Nicht selten war ein Drittel des IT-Personals für den „operativen Betrieb“ zuständig, d. h. für die Wartung der Rechenzentren, die Beschaffung neuer Hardware, die Bereitstellung von neuen Servern und Software sowie die Außerbetriebnahme veralteter Hardware, die Netzwerkverwaltung, die rechtzeitige Anwendung von Systemsoftwarepatches, das Debuggen von Routerschleifen und andere ähnlich obskure Aufgaben.

Damals wie heute war den meisten CIOs zudem intuitiv bewusst, dass die Anforderungen an Unternehmensanwendungen weitgehend saisonbedingt sind. Zur Verwaltung des Hauptbuchs des Unternehmens verwendete Enterprise Resource Planning-Systeme (ERP) werden zum Ende des Quartals und Geschäftsjahrs am meisten genutzt. Performancemanagement-Systeme für Mitarbeitergespräche werden während des Prüfungszeitraums intensiv genutzt, haben im restlichen Jahr aber praktisch keine Verwendung. Die „Faustregel“ vieler IT-Manager war es, das Drei- oder Vierfache der Menge an Hardware für die erwartete Workload zu kaufen – um sicherzustellen, dass Anwendungen niemals während der Spitzenzeiten ausfallen.

Die Folge war natürlich, dass die durchschnittliche CPU-Auslastung im Rechenzentrum mitunter im einstelligen Bereich blieb. Durch Virtualisierung – die Bereitstellung mehrerer Workloads auf einem einzigen Server – konnte die Auslastung zwar in einem gewissen Ausmaß verbessert werden, doch insgesamt blieb sie gering. Dies ließ darauf schließen, dass Geld für IT-Ressourcen verschwendet wurde, die noch immer nicht voll ausgelastet wurden.

Eine IT-Abteilung konnte leicht 80 Prozent oder mehr ihres Budgets für operative Mitarbeiter, die Verwaltung von Investitionsgütern und die Softwarewartung ausgeben, sodass nur wenig Mittel für Innovation übrigblieben. Da in der Regel jede IT-Investition die für das Wachstum des Unternehmens verfügbaren Mittel schmälerte, verwundert es daher kaum, dass CEOs und CFOs ständig auf der Suche nach Möglichkeiten zur Kürzung des IT-Budgets waren.

Es musste sich etwas ändern.

Wirtschaftlichkeit der Cloud

Kurz nach der Jahrhundertwende begannen mehrere Technologieanbieter Computing-Dienste zu vermieten – die Geburtsstunde der Cloud. Schon schnell wurde klar, dass dieses Modell Unternehmenskunden erhebliche Vorteile bot.

Beim Cloud Computing bezahlen Unternehmen für das, was sie nutzen – wie bei einem Telekommunikationsanbieter. Wenn die Nachfrage sinkt und Sie keine Kapazität mehr benötigen, können Sie die Systeme abschalten und müssen nichts bezahlen. Dieses einfache Modell steht in krassem Gegensatz zum gerade beschriebenen *traditionellen, kapitalintensiven* Enterprise-Computing-Modell.

Die Cloud ist durch die Abonnementbasis ein *Betriebskostenmodell*. In der Cloud wird Computing zu einem Service, der Kunden monatlich in Rechnung gestellt wird. Im Gegensatz zu vielen anderen Diensten basiert die Abrechnung auf der Nutzung. Je mehr Computing-, Netzwerk- und Speicherressourcen Sie benötigen, umso höher fällt die Rechnung aus. Selbstverständlich gilt auch das Gegenteil: Je weniger Sie nutzen, umso weniger müssen Sie bezahlen. In der Tat schwankt in den meisten IT-Organisationen die Systemauslastung: Manche Anwendungen (z. B. Einzelhandel) sind saisonal, andere (z. B. Schulungsanwendungen) laufen nur eine bestimmte Zeit, bevor sie wieder abgeschaltet werden, und wieder andere sind einfach nicht prognostizierbar. Durch das nutzungsbasierte Modell ist die Cloud die perfekte Lösung für Schwankungen dieser Art (siehe Abbildung 1-1).

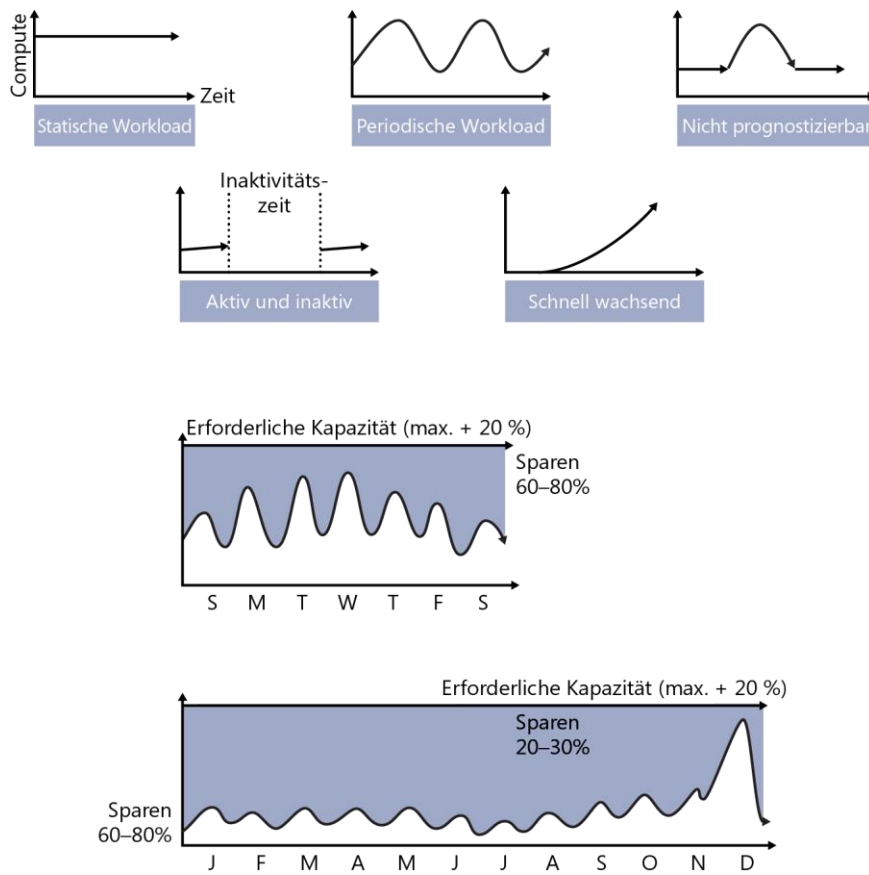


Abbildung 1-1: Häufige Modelle der Anwendungsauslastung

(Erwähnenswert ist, dass in On-Premises-Rechenzentren wie gesagt die *maximale* Auslastung geplant und bereitgestellt werden muss, wodurch die Kosten im Vergleich zur Cloud deutlich höher sind.)

Das ist jedoch noch nicht alles. Der Betrieb in der Cloud befreit Unternehmen von banalen Aufgaben wie Systemsicherung, Netzwerkwartung, Patches und Softwareupgrades, da dafür der Cloud-Anbieter zuständig ist. Der Cloud-Anbieter wiederum hat großes Interesse daran, Best Practices für die Systemwartung einzusetzen, und leistet in vielen Fällen sogar Pionierarbeit in diesem Bereich. Die Vorteile werden direkt an den Kunden weitergegeben.

Cloud-Anbieter wie Microsoft können darüber hinaus Skaleneffekte erzielen, da sie Hardware in großen Stückzahlen kaufen, z. B. 10.000 Server auf einmal. Sehr große Rechenzentren, die Public Clouds hosten, können zudem durch den Kauf anderer Ressourcen profitieren: Für Cloud-Rechenzentren wird nur ein Viertel der durchschnittlichen Stromkosten in den USA fällig. In vielen Fällen nutzen Cloud-Rechenzentren lokale erneuerbare Energien. Das Microsoft-Rechenzentrum in Quincy, Washington, befindet sich beispielsweise in der Nähe eines Wasserkraftwerks, und andere Rechenzentren arbeiten mit Windstrom und anderen umweltfreundlichen Energiequellen.

In Abbildung 1-2 sehen Sie, wie die Gesamtbetriebskosten pro Server bei steigender Anzahl drastisch sinken.

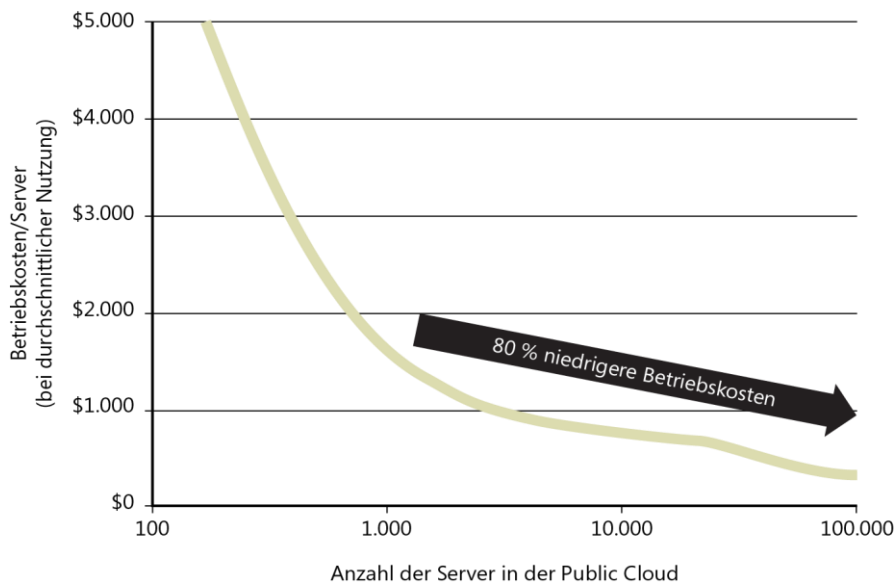


Abbildung 1-2: Skaleneffekte in der Cloud

Diese Einsparungen können (und werden) wiederum an Kunden des Cloud-Dienstes weitergegeben (werden).

Später werden wir erörtern, wie IT-Abteilungen die durch Cloud Computing zu erwartenden Einsparungen quantifizieren können.

Am wichtigsten ist wohl, dass sich bei der Cloud nicht die „entweder/oder“-Frage stellt. Sicher ist es möglich und in vielen Fällen erstrebenswert, einige Anwendungen in einem lokalen, traditionellen Rechenzentrum auszuführen, während andere zur Cloud migriert werden. Anbieter wie Microsoft haben große Investitionen in dieses *Hybrid Cloud*-Modell getätigt, das Cloud-Anwendungen sicher mit Anwendungen im Rechenzentrum eines Kunden vernetzt. Wie wir sehen werden, bietet das Hybridmodell Unternehmen die Möglichkeit, ihre Anwendungen *in ihrem eigenen Tempo* zur Cloud zu migrieren.

Wenn ein On-Demand-Computing-Service verfügbar ist, werden auch viele andere Arten der Effizienzsteigerung möglich. Eigene Systeme für Anwendungsentwicklung und -tests stellen beispielsweise häufig einen großen Kostenaufwand für IT-Abteilungen dar und sind letzten Endes doch nicht von direktem Nutzen für die Anwender. Mit der Cloud können Entwickler und Tester schnell cloudbasierte Ressourcen zuweisen, für ihre Arbeit einsetzen und herunterskalieren, wenn sie nicht mehr benötigt werden. Durch die großen Mengen an günstigem Speicher in der Cloud stellt die Datensicherung in der Cloud (und, falls erforderlich, an mehreren geografischen Standorten) eine unkomplizierte und kostengünstige Lösung dar. Wir werden uns in diesem Buch noch ausführlicher mit diesem Aspekt befassen.

Nach den Gesamtbetriebskosten (TCO): Der Weg zur Cloud geht weiter

Viele Unternehmen, mit denen wir gesprochen haben, sind der Meinung, dass die Migration zur Cloud ihnen hilft, Geld zu sparen und effizienter zu arbeiten (dem stimmen wir zu). In Kapitel 7 werden wir uns damit befassen, wie Unternehmen die Nutzung der Cloud nach dem Umstieg von Tag zu Tag optimieren und den Verbrauch sowie die Nutzung zum Erreichen ihrer Kostenziele anpassen können.

Doch das ist nur die halbe Geschichte. Wie mittlerweile viele Unternehmen feststellen, ist der Wunsch der Kostensenkung in Wirklichkeit nur der erste Schritt auf einem Weg.

Die Cloud eröffnet eine Vielzahl von Innovationsmöglichkeiten, die nicht nur die IT verbessern, sondern von direktem Nutzen für das Unternehmen sind. Dank der Cloud ist der CIO nicht mehr nur eine Kostenstelle, sondern kann aktiv dazu beitragen, das Wachstum des Unternehmens voranzutreiben.

Im Jahr 2016 beauftragte Microsoft Forrester Consulting mit der Durchführung einer unabhängigen Studie¹ zum Return on Investment (ROI) der Nutzung der Cloud. Schwerpunkt der Studie war die PaaS-Nutzung (Platform as a Service), auf die wir in Kapitel 2 ausführlicher eingehen, die Ergebnisse waren aber dennoch beeindruckend: Unter anderem wurden ein ROI von 466 Prozent und eine Verringerung des IT-Zeitaufwands für die Wartung um 80 Prozent erzielt:

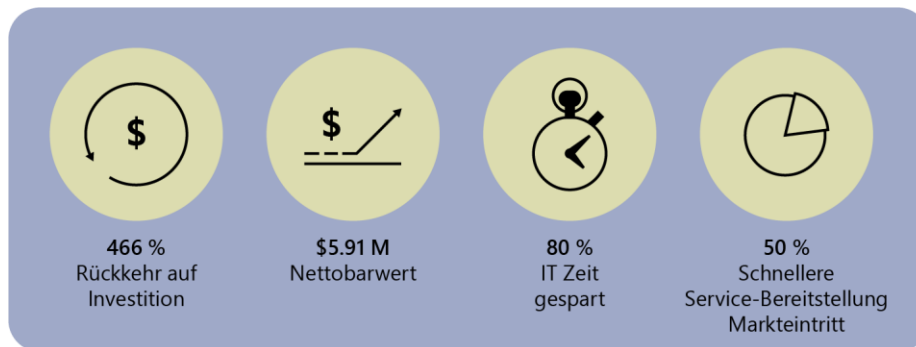


Abbildung 1-3: Vorteile des Cloud Platform-as-a-Service

Die Ergebnisse können sich natürlich je nach Fall unterscheiden, und in Teil II dieses Buchs werden wir uns sehr viel ausführlicher mit der Quantifizierung der Cloud-Kosten und Kosteneinsparungen befassen. Der springende Punkt ist jedoch, dass die deutliche Reduzierung nicht wertschöpfender Aufgaben (z. B. Wartung von Servern und Patchverwaltung) Unternehmen in die Lage versetzt hat, ihre IT-Ressourcen für *geschäftliche Innovation* einzusetzen.

Innovation

Letzten Endes ist es das Ziel jeder Unternehmensstrategie, sich von der Konkurrenz abzuheben und Wettbewerbsvorteile zu erlangen, und es besteht kaum noch Zweifel daran, dass sich die IT zu einem entscheidenden Element der modernen Strategie entwickelt hat. Die IT bringt die transformative Innovation voran und ermöglicht es Unternehmen, sich durch die Instanziierung von Prozessen, die laufend Wettbewerbsvorteile verschaffen, erfolgreicher im Wettbewerb zu behaupten.

Wie wir sehen werden, läutet die Entwicklung einer globalen Computing-Cloud ein völlig neues Maß an Innovation in Anwendungen und Märkten ein. Diese neuen Formen der Innovation können eine Organisation und ein Unternehmen *verwandeln*.

Transformative Innovation fördert eine andere Kultur und Einstellung, als die meisten Unternehmen derzeit haben. Da sowohl IT als auch Unternehmensleitung betroffen sind, erfordert diese Kultur eine enge Zusammenarbeit zwischen diesen beiden Bereichen.

Auf den nächsten Seiten untersuchen wir mehrere kurze Fallstudien von verschiedenen globalen Unternehmen, die alle von der Nutzung der Cloud profitiert haben.

¹ „The Total Economic Impact of Microsoft Azure PaaS“, Juli 2016

AccuWeather

AccuWeather, ein weltweit führender Anbieter von Wettervorhersagen, benötigte eine bessere Lösung zur Verarbeitung von mehr als 4 Milliarden Datenanfragen pro Tag. AccuWeather nutzt die Cloud zur Entwicklung und für Machbarkeitsstudien – eine einfache Aufgabe, da dank der Cloud keine Hardware gekauft und bereitgestellt werden muss.

Das Unternehmen erreichte zudem On-Demand-Skalierbarkeit, verbesserte den Zugriff auf Echtzeitwetterdaten und senkte seine Kosten um bis zu 40 Prozent.

Skalierbarkeit war für das Unternehmen besonders wichtig: „Als weltweit immer mehr vernetzte Geräte auf den Markt kamen, stieg die Anzahl unserer täglichen Anfragen innerhalb von fünf Jahren von 2 Millionen auf mehr als 4 Milliarden“, so Chris Patti, Vice President of Technology bei AccuWeather. „Die Skalierung entwickelte sich zu einer Herausforderung.“ Und innerhalb weniger Jahre vervierfachte sich das Volumen auf 17 Milliarden Anfragen pro Tag.

Beim Wetter geht es natürlich um Daten. Das Unternehmen nutzt Funktionen für Analytics und künstliche Intelligenz in der Cloud (Microsoft Cortana Intelligence Suite) zur Integration von Verkaufsdaten und Wetterinformationen. In einem kürzlichen Projekt mit Starbucks half AccuWeather dem Kaffeeriesen, saisonale Probleme wie das Knappwerden von Eis und Bechern bei heißem Wetter zu lösen. Ein weiteres Beispiel ist ein globaler Süßwarenhersteller, dem es AccuWeather ermöglichte, die meistverkauften Produkte sowie Zusammenhänge zwischen Verkaufsspitzen und dem Wetter zu ermitteln.

Kurz gesagt: Durch die Nutzung der Cloud fand AccuWeather heraus, was viele Unternehmen bereits entdeckt haben oder in Kürze entdecken werden – die Cloud kann Ihnen Geld sparen und neue Märkte erschließen.

GEICO

GEICO, ein seit 1936 etablierter Kfz-Direktversicherer, der heute der zweitgrößte Anbieter privater Kfz-Versicherungen in den Vereinigten Staaten ist, verstärkt seine digitale Präsenz, um die Beziehung zu Kunden über mehrere digitale Kanäle zu verbessern. Fikri Larguet, Director of Cloud Services bei GEICO, bemerkt unter Bezugnahme auf die zunehmende Nutzung des mobilen Internets und die drastische Verbreitung von sozialen Medien dazu Folgendes:

In den letzten fünf bis acht Jahren hat das Interesse der Kunden an digitaler Interaktion enorm zugenommen. Kunden interagieren sehr viel häufiger und auf neuen, interessanten Wegen mit uns. Wir wollen der Zeit bei der Nutzung neuer Möglichkeiten zur digitalen Interaktion einen Schritt voraus sein.

Aber was bedeutet digitale Interaktion? Es bedeutet, rund um die Uhr und auf jedem Gerät überall für den Kunden verfügbar zu sein.

Wie AccuWeather stellte auch Geico fest, dass das Unternehmen durch die Umstellung auf ein Cloud-Modell all seine Kunden jederzeit und in beliebigem Umfang mühelos erreichen kann. Zudem nahmen die IT-Kosten in vielen Bereichen ab: Durch die Einführung eines DevOps-Modells (siehe Kapitel 7) in Verbindung mit der Cloud-Entwicklung konnten Entwicklungsteams ihre Arbeit beschleunigen. Da die Cloud die Möglichkeit bietet, mehrere Kopien von Anwendungen in verschiedenen Rechenzentren auszuführen, werden Redundanz- sowie Business Continuity-/Disaster Recovery-Vorgänge (BC/DR) deutlich vereinfacht – und dies sind wie gesagt Vorteile, von denen jedes Unternehmen profitieren kann.

Rolls-Royce

Weltweit sind über 13.000 kommerzielle Luftfahrzeugtriebwerke von Rolls-Royce im Einsatz. Seit 20 Jahren bietet das Unternehmen umfassende Wartungsdienste für die Motoren, damit die Luftfahrzeuge stets einsatzbereit sind und effizient funktionieren. Allerdings wird es für Fluggesellschaften immer schwieriger, die rasant steigende Datenmenge aus unterschiedlichsten Flugzeugteilen effektiv zu analysieren und Insights daraus zu gewinnen. Daher setzt Rolls-Royce auf die Microsoft Azure-Plattform, um mithilfe von Daten seinen Kundenservice zu verbessern.

Rolls-Royce nutzt die Skalierbarkeit und On-Demand-Bereitstellung von Analytics (siehe Kapitel 12) in Azure sowie die Funktionen für künstliche Intelligenz (siehe Kapitel 13) zur Datenmodellierung und -analyse in großem Maßstab, um operative Anomalien präzise zu erkennen und Kunden bei der Reaktionsplanung zu unterstützen. Nick Farrant, Senior Vice President von Rolls-Royce, äußert sich dazu wie folgt:

Terabytes an Daten von großen Flugzeugflotten müssen verarbeitet und analysiert werden, und bei diesen Daten sprechen wir nicht von Kilobytes, sondern von Gigabytes pro Stunde. Die Funktionen von Microsoft Cortana Intelligence helfen uns, in großen Datenmengen das Wichtige vom Unwichtigen zu trennen, sodass wir uns auf die wirklich wertvollen Daten konzentrieren können. Unsere Vision der zukünftigen digitalen Fähigkeiten wird die Aggregation vieler Datenquellen und die Bereitstellung einer Plattform für die Zusammenarbeit mit Kunden erfordern.

Aufgrund der bemerkenswerten Technologien, die heute verfügbar sind und es Unternehmen ermöglichen, große Mengen von Daten über ihre Kunden, Partner und Geräte zu erfassen, glauben wir, dass in Zukunft jedes Unternehmen datengesteuert sein wird. Wegen der damit verbundenen Vorteile für ihre Unternehmen sollten CIOs und IT-Entscheidungsträger Daten, Analytics und künstliche Intelligenz in ihre Cloud-Pläne einbeziehen.

Brainshark

Brainshark ist eine cloudbasierte Verkaufsschulungs- und -vorbereitungsplattform, mit deren Hilfe Vertriebsmitarbeiter ihre Fähigkeiten in der Präsentation von Verkaufsmaterialien für Kunden perfektionieren können. Sie reduziert die Kosten und den Ressourcenaufwand für Schulungen und maximiert die Effektivität von Verkaufsgesprächen.

Mit einem Kundenstamm, zu dem die Hälfte der Fortune-100-Unternehmen zählt, ist Brainshark auf seinem Gebiet ein klarer weltweiter führender Anbieter. Kontinuierliche Innovationen und Verbesserungen haben dafür gesorgt, dass das Unternehmen seine Führungsposition über die gesamten 17 Jahre seines Bestehens aufrechterhalten konnte und den Markt auch weiterhin dominieren wird.

Brainshark begann mit der Nutzung der Cloud, indem es all seine Videoschulungsmaterialien in der Cloud speicherte. Dazu Michael Ferioli, Vice President of Engineering, von Brainshark:

Durch das Speichern von Videos auf Azure entfielen der Verwaltungsaufwand und die bisherigen Kosten für die Wartung fast vollständig. Tatsächlich sind unsere laufenden Kosten bei Microsoft niedriger als wir dachten. Seit mehr als zwei Jahren habe ich kein einziges Hardwaregerät mehr gekauft.

Und wie hat das Unternehmen seine Kosteneinsparungen genutzt? Es begann, neue innovative Methoden für umfassende Verkaufsschulungen zu entwickeln. Beispielsweise erstellte Brainshark mit dem fortschrittlichen Augmented Reality-Gerät HoloLens von Microsoft realistischere Schulungsszenarien. Schulungsteilnehmer können durch Microsoft HoloLens ein simuliertes Kundengespräch erleben, komplett mit Präsentationsfunktionen und lebensechten Avataren, die die Kunden repräsentieren. Im Gegensatz zu Virtual Reality-Technologien kombiniert HoloLens reale Räume mit virtuellen Elementen, sodass Teilnehmer das Verkaufstraining an Orten durchführen können, mit denen sie vertraut sind.

Durch die Reduzierung der bei einem On-Premises-Rechenzentrum anfallenden Kosten für nicht wertschöpfende Funktionen konnte Brainshark echte Innovationen schaffen und sich mit bemerkenswerten neuen Methoden von der Konkurrenz absetzen.

Katastrophenhilfe: Oso (Washington) 2014 und Nepal 2015

Da die Cloud die IT in die Lage versetzt, Anwendungen sehr schnell zu erstellen und in Betrieb zu nehmen, wird sie von Disaster Recovery-Teams auf der ganzen Welt genutzt, um rasch Hilfe für Menschen in Not zu leisten.

Am 22. März 2014 stürzte nach starken Regenfällen ein Hang auf die kleine Stadt Oso im Bundesstaat Washington im Nordwesten der USA. Häuser wurden zerstört, und 43 Menschen starben. In der Folgezeit brachen die Vertreter von fast 200 staatlichen Einrichtungen und Hilfsorganisationen, darunter das Rote Kreuz, die Federal Emergency Management Agency, die Nationalgarde von Washington und das Such- und Rettungsteam der US-Marine, sowie Tausende von Vertretern der Medien über Oso herein.

Da die Dokumentation- und Koordinationssysteme der örtlichen Behörden schnell überlastet waren, migrierte Microsoft Services Disaster Response die Aufzeichnungen und Daten der Stadt Oso mit Unterstützung des Azure-Produktteams zur Cloud. Dank der nahezu unbegrenzten Kapazität der Cloud konnte jeder, der Zugriff auf die Aufzeichnungen benötigte, schnell und effizient nach Daten suchen und sie abrufen. Mit Microsoft Office 365 stellte das Team zudem in kürzester Zeit ein Incident Command System bereit, über das sich die Einsatzleiter und Vertreter der verschiedenen Organisationen miteinander vernetzen konnten.

Ein Jahr später wurden bei einem gewaltigen Erdbeben in Nepal 600.000 Gebäude dem Erdboden gleichgemacht und Tausende von Menschen getötet. Danach stand das abgelegene Bergland vor der schwierigen Aufgabe des Wiederaufbaus. „Katastrophenhilfe ist immer eine überwältigende Aufgabe“, sagte damals Dan Strobe, Projektmanager für das [United Nations Development Program](#) (UNDP). „Es gibt zu viel zu tun, zu viele Menschen, die Hilfe benötigen, und niemals genügend Zeit oder Ressourcen.“

Die gewaltige Aufgabe des Wiederaufbaus begann mit der Kartierung der ursprünglichen Gebäude. In der Vergangenheit wurden solche Aufzeichnungen in Papierform geführt. Zur Beschleunigung des Wiederaufbaus erstellte das [Microsoft Innovation Center](#) in Nepal eine Mobiltelefonanwendung (Abbildung 1-4), mit der die Arbeiter vor dem Beseitigen der Trümmer über das GPS eines Geräts den Grundriss eines beschädigten Hauses erfassen und in der Cloud speichern konnten. Um die Wirtschaft wieder anzukurbeln, wurden über die App auch die täglichen Barzahlungen an die Arbeiter verwaltet. Cloudanwendungen wie Office 365 und das Microsoft-Datenvisualisierungstool [Power BI](#) halfen den Beteiligten bei der Koordination und Verfolgung der Fortschritte.



Abbildung 1-4: Verwaltungsanwendung für die Trümmerbeseitigung in Nepal

Erkenntnisse

Was haben wir gelernt? Diese Beispiele veranschaulichen das Potenzial der Cloud. Wir haben erkundet, wie Kunden durch die Cloud Folgendes ermöglicht wird:

- Entwicklung und schnelle Bereitstellung von Anwendungen mit einer Reichweite und in einem Ausmaß, das in ihren eigenen Rechenzentren unmöglich gewesen wäre
- Kommunikation mit internetfähigen Geräten rund um den Globus
- Einblicke in Big Data und Analytics-Dienste für Personalisierung, bessere Produkte und effizientere Prozesse
- Unübertroffene Entwicklungs-, Test-/Experimentier- und Innovationszyklen

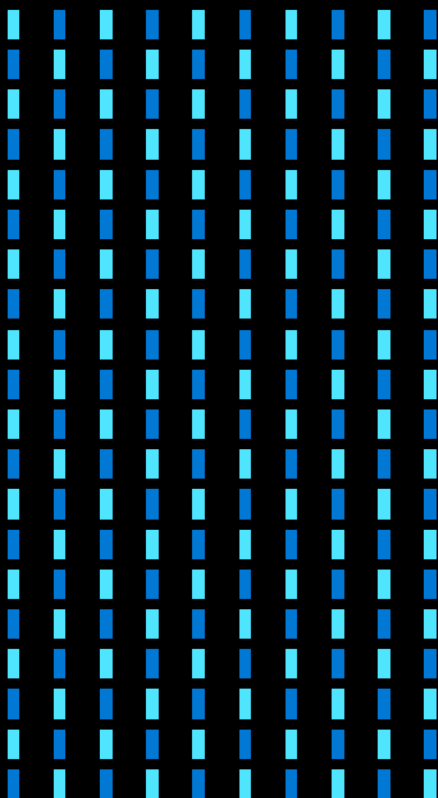
Jede IT-Abteilung muss die Informationsressourcen ihres Unternehmens schützen, die Kosten reduzieren und sich um den täglichen Geschäftsbetrieb kümmern. Diese Funktionen sind und werden immer wichtige Komponenten jeder IT-Organisation sein. Die IT muss jedoch auch Innovation ermöglichen und fördern, um vorhandene Prozesse schneller und günstiger auszuführen und neue Geschäftsmodelle zu unterstützen.

Mit der Cloud verlagert sich die Balance zwischen Wartung und Innovation. Wie wir sehen werden, bietet der Betrieb in der Cloud viele Kostenvorteile, die es IT-Abteilungen ermöglichen, sich auf die Innovation zu konzentrieren. Durch den Betrieb in der Cloud werden Vorgänge wie System software upgrades und -patches überflüssig, und das IT-Team kann sich auf Aktivitäten konzentrieren, die Umsatz generieren. Neue Möglichkeiten in der Cloud ermöglichen auch neue Arten von leistungsstarken Anwendungen. Wie wir in den Beispielen zuvor gesehen haben, sehen immer mehr Unternehmen die Cloud als Möglichkeit an, um Innovation im Unternehmen zu beschleunigen und sich von der Konkurrenz abzuheben.

Wie bei jeder großen technologischen Änderung erstreckt sich auch diese Art von Transformation auf mehr als nur Technologie. Auch Veränderungen bei der Unternehmenskultur, den Unternehmens- und IT-Prozessen, individuellen Rollen, Governance und Technik sind erforderlich. Wie Unternehmen diese Transformation umsetzen, erfahren Sie im Rest dieses Buchs.

Kapitel 2

Was ist die Cloud?



Wie jede neue Technologie bringt die Cloud eine ganze Reihe neuer Begriffe, Akronyme und Abkürzungen mit sich. Um die richtigen Entscheidungen bezüglich der Nutzung der Cloud treffen zu können, ist es jedoch wichtig, die verschiedenen Formen von Cloud Computing zu verstehen. In diesem Kapitel untersuchen wir die verfügbaren Formen der Cloud und, wie Sie diese beim Enterprise-Computing nutzen können.

Was also ist die Cloud?

In ihrem Kern besteht die Cloud aus Millionen von Servern, die auf mehrere sehr große Rechenzentren an strategischen Standorten auf der ganzen Welt verteilt sind. Alle Cloud-Anbieter verwenden spezielle Serverhardware, die die Kosten senken, die Umweltbilanz verbessern und natürlich maximale Rechenleistung bieten soll.

Die Rechenzentren, in denen sich die Server befinden, sind für maximale Effizienz und minimale Umweltbelastung ausgelegt. Zahlreiche Forschungsarbeiten widmen sich der Verbesserung der Umweltfreundlichkeit von Rechenzentren. Das Rechenzentrum von Microsoft in Quincy, Washington, befindet sich beispielsweise neben einem Wasserkraftwerk am Columbia River und ist ein gutes Beispiel dafür, wie Cloudanbieter lokale Möglichkeiten nutzen, um ihre CO₂-Bilanz zu verbessern. Rechenzentren in kühleren Klimazonen nutzen anstelle von Klimaanlage Umgebungsluft, um den Stromverbrauch zu reduzieren. Einige Anbieter verwenden Windkraft, und andere nutzen kostengünstigeres Brauchwasser in den Klimaanlage, sofern dies notwendig ist.

Ein wichtiger Maßstab für die Effizienz eines Rechenzentrums ist die Power Usage Effectiveness (PUE), mit der die Nutzung von Energie im Rechenzentrum gemessen wird. Ein perfektes PUE-Ergebnis ist 1,0. Bei diesem Wert wird die gesamte Energie für die Hard- und Software genutzt (formal ist die PUE definiert als der gesamte Energieverbrauch einer Einrichtung dividiert durch den Energieverbrauch von IT-Geräten). Traditionelle Unternehmensrechenzentren erzielen in der Regel einen PUE-Wert von 2,0, was bedeutet, dass die Hälfte der Energie von anderen Geräten verbraucht wird, z. B. Klimaanlage, Beleuchtung usw. Cloudrechenzentren erreichen heute PUE-Werte von 1,1 und noch weniger. Diese Ergebnisse sind den erheblichen Investitionen und Innovationen seitens der Cloudanbieter zu verdanken.

Public, Private und Hybrid Clouds

In den folgenden Unterabschnitten erläutern und untersuchen wir die drei großen Cloud-Modelle.

Private Cloud

Als Erstes wollen wir die Unterschiede zwischen „Private“ und „Public“ Clouds erörtern.

Der Begriff *Private Cloud* wird oft falsch verwendet. Manche werden sagen, dass eine Private Cloud nichts anderes ist als ein traditionelles On-Premises-Rechenzentrum. In Wirklichkeit unterscheiden sich diese beiden Modelle jedoch erheblich. Beim traditionellen On-Premises-Modell kaufen IT-Abteilungen Hardware, wenn diese für Anwendungen erforderlich ist, und oft unterscheiden sich die in einem Jahr angeschafften Server hinsichtlich Aussehen und Verhalten erheblich von denen des Vorjahrs. Darüber hinaus arbeiten IT-Abteilungen herkömmlicherweise mit einer Mischung von Hard- und Software – vom Mainframe bis zum PC-Server – mit einer Vielzahl von Betriebssystemen, Datenbanken und anderer Systemsoftware. Das Konzept von On-Demand-Computing, das das Hauptmerkmal der Cloud ist, ist aus diesen Gründen nicht möglich.

In einer Private Cloud werden spezifische Technologien des Cloudmodells in einem On-Premises-Rechenzentrum gehostet, in dem auf einer großen Zahl von Standardhardwarekomponenten identische Systemsoftware ausgeführt wird. Anders gesagt: eine „Cloud“, die Ihnen gehört. Private Clouds können nützlich sein, da sie dieselbe Technologie implementieren können wie die Public Cloud. Dies kann in Szenarien erforderlich sein, in denen bestimmte Anwendungen oder Daten das Gelände nicht verlassen dürfen (in Kapitel 6 erörtern wir die Gründe, die gegen die Public Cloud sprechen).

Private Clouds sind jedoch von sehr begrenztem Nutzen. Private Clouds können nicht mit den Kostenvorteilen und der Effizienz der Public Cloud mithalten, da sie ein beachtliches Kapitalbudget und ein operatives Team erfordern (Posten, die folglich weiterhin in Ihrer Unternehmensbilanz erscheinen). Darüber hinaus können einzelne Unternehmen nicht die zuvor erwähnten Skaleneffekte eines Public Cloud-Anbieters erzielen, wodurch ihre Kosten proportional höher sind.

Public Cloud

Eine *Public Cloud* – um die es in diesem Buch vorrangig geht – wird von einem großen Technologieanbieter, der Computing, Speicher und Software auf Mietbasis zur Verfügung stellt, erstellt, verwaltet und gewartet. Die führenden Public Cloud-Anbieter besitzen Rechenzentren auf der ganzen Welt, in denen buchstäblich Millionen von Servern zur Verwendung verfügbar sind. Kunden (Unternehmen) können sich entweder Anwendungen zu Nutze machen, die bereits in der Cloud vorhanden sind, oder ihre eigenen proprietären Anwendungen hochladen. Wie wir sehen werden, gibt es eine Reihe von Möglichkeiten, Anwendungen physisch in der Cloud bereitzustellen, aber wie private Anwendungen des Unternehmensnetzwerks wirken zu lassen.

Hybrid Cloud

Oft möchte ein Unternehmen einige seiner Anwendungen auf den On-Premises-Systemen belassen und andere in die Public Cloud verschieben. Dabei ist es natürlich wünschenswert, dass all diese Anwendungen weiterhin wie zuvor funktionieren, d. h. als wären sie noch immer lokal und im selben Netzwerk. Wenn einige Anwendungen in der Cloud und andere lokal bereitgestellt werden, wird dies als *Hybrid Cloud* bezeichnet. Jedes Unternehmen wird zu irgendeinem Zeitpunkt eine Hybrid Cloud haben. Auch wenn es plant, irgendwann alle Anwendungen zur Cloud zu migrieren, wird es während der Übergangsphase einen Zeitpunkt geben, zu dem einige Anwendungen verschoben wurden und andere noch nicht: ein Hybridmodell.

Zum sicheren Verbinden der beiden Umgebungen sind mehrere Lösungen verfügbar. Sie können ein virtuelles privates Netzwerk (VPN) einrichten, sodass der Eindruck entsteht, dass sich die Cloud-Anwendungen im internen Unternehmensnetzwerk befinden. Sie können VPNs einzeln für jede Anwendung oder mit einem Hardwaregerät für die gesamte Unternehmensinfrastruktur bereitstellen.

Alternativ können Unternehmen über ihren Telekommunikationsanbieter eine Standleitung erwerben, die das Unternehmensrechenzentrum mit der Cloud verbindet. Bandbreite kann in diesem Fall nach Bedarf gekauft werden. Diese Lösung ist vorzuziehen, wenn sämtlicher Datenverkehr vom öffentlichen Internet getrennt werden soll oder eine wesentlich höhere Bandbreite erforderlich ist. Sie bringt aber natürlich zusätzliche Kosten mit sich.

Skalierbarkeit macht Computing zu einem On-Demand-Service

In der Cloud kann Computing *skaliert* werden, d. h. die Computing-Ressourcen werden entsprechend den Anforderungen angepasst. Skalierbares bzw. Hyperscale Computing erfordert, dass alle Computing-Funktionen, die Sie benötigen, sofort und jederzeit verfügbar sind. Wenn Sie für eine nächtliche Big Data Analytics nur für einige Stunden 10.000 Server benötigen, stehen Ihnen diese Server zur Verfügung, und sobald Sie den Auftrag abgeschlossen haben, können Sie sie wieder freigeben. Skalierbarkeit setzt auch Konfigurierbarkeit (und Rekonfigurierbarkeit) in großem Maßstab voraus. Je nach Wunsch des Kunden könnte ein Server heute einer bestimmten Echtzeitanwendung mit sehr hoher Vereinbarung zum Servicelevel (SLA) zugewiesen werden und morgen einer Hintergrundaufgabe mit einer ganz anderen SLA.

Skalierbarkeit bedeutet auch, dass die Rechenleistung überall auf der Welt mit ähnlicher Latenz verfügbar ist. Dies wiederum bedeutet, dass Cloud-Anbieter rund um die Welt riesige Rechenzentren errichten müssen (was sie auch getan haben). Die globale Dimension der Public Cloud ermöglicht im Gegenzug beliebig viele neue Funktionen, z. B. die Möglichkeit zur geografischen Verteilung von Daten und eines regionsübergreifenden Failovers, um nur zwei zu nennen.

Hyperscale Computing bietet somit deutlich mehr Potenzial – Funktionen und Wirtschaftlichkeit – als ein Unternehmensrechenzentrum.

Aufgrund dieser unglaublichen globalen Ausmaße kann Computing *as a Service* bereitgestellt werden. Dies bedeutet, dass die Cloud eine Reihe von Funktionen bietet, die Unternehmen mieten und für einen bestimmten Zeitraum nutzen können. Je nach Bedarf können sie dann weitere Funktionen hinzufügen und ihre Verwendung wieder einstellen, wenn die Funktionen nicht mehr benötigt werden. Wie erwähnt, funktioniert dieses Modell natürlich ähnlich wie viele andere gebräuchliche Services, z. B. Telekommunikation, Strom usw.: Sie zahlen für das, was Sie tatsächlich nutzen, und nicht mehr.

„As a service“

Wie wir bereits erwähnten, wird Computing in der Cloud als Service zur Verfügung gestellt, und es gibt drei vorherrschende Anwendungsmodelle für Cloud Computing. Im Folgenden werden wir uns jedes dieser Modelle genauer ansehen.

Infrastructure as a Service

Beim Infrastructure-as-a-Service-Modell (IaaS – ausgesprochen „eye-as“) mieten Sie nur die Serverhardware und eine kleine Menge an Software (den Hypervisor) zum Hosten der virtuellen Maschine (VM) Ihrer Anwendung, wobei die VM aus dem Betriebssystem, der zugehörigen Systemsoftware und der Anwendung selbst besteht. IaaS bedeutet, dass VMs einfach von On-Premises-Systemen in die Cloud *verschoben* werden. Abbildung 2-1 zeigt, dass auf einem Cloud-Server viele Betriebssysteme und Anwendungen gleichzeitig gehostet werden können. Ein kleines als *Hypervisor* bezeichnetes Stück Code sorgt dafür, dass alle Anwendungen und Betriebssysteme rechtzeitig und effizient ausgeführt werden.

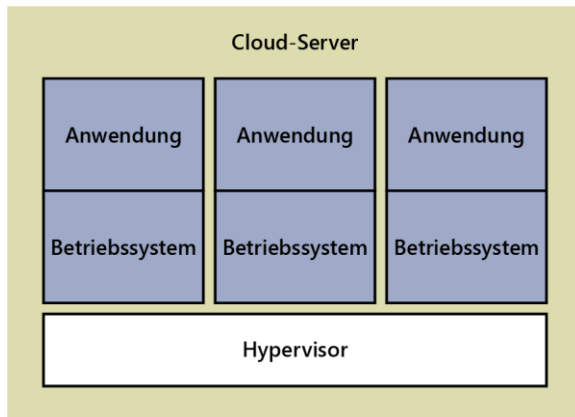


Abbildung 2-1: Infrastructure as a Service

Anders ausgedrückt: Sie beschaffen – und pflegen – die in Abbildung 2-1 blau hervorgehobenen Komponenten.

Dies ist die einfachste und schnellste Migrationsstrategie und bietet viele Vorteile wie Kosteneinsparungen. Dennoch muss Ihr Team Aufgaben wie Patchverwaltung, Updates und Upgrades ausführen. Nichtsdestotrotz zählt IaaS zu den häufigsten Cloud-Bereitstellungsmustern, da nur sehr wenig Zeit zwischen Erwerb und Bereitstellung verstreicht. Da das Modell die größte Ähnlichkeit zum heutigen IT-Betrieb aufweist, ermöglicht es einen einfachen Einstieg in die moderne IT-Kultur und die zugehörigen Prozesse. Wie wir sehen werden, kommt beim Großteil der Migration und vor allem in den frühen Phasen der Einführung der Cloud das IaaS-Modell zum Einsatz.

Platform as a Service (PaaS)

Beim Platform-as-a-Service-Modell (PaaS – ausgesprochen „pahz“) wird sämtliche Systemsoftware vom Cloud-Anbieter gewartet, sodass die IT-Abteilung sich nicht mehr um Upgrades und Patches kümmern muss. Bei einem PaaS-Bereitstellungsmodell (Abbildung 2-2) ist das Unternehmen lediglich für die Bereitstellung des Codes auf den PaaS-Geräten zuständig: Der Cloud-Anbieter stellt sicher, dass Betriebssysteme, Datenbanksoftware, Integrationssoftware und andere Funktionen gewartet und aktuell gehalten werden und eine hohe Vereinbarung zum Servicelevel (SLA) erreichen.

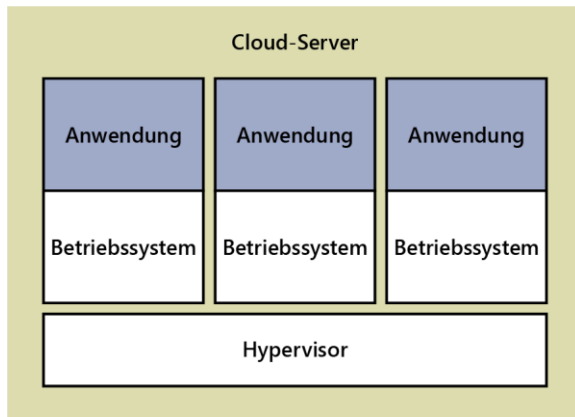


Abbildung 2-2: Platform as a Service

Beachten Sie, dass es sich in Abbildung 2-2 bei den blauen Komponenten – den Komponenten, die der Benutzer beschaffen und pflegen muss, – *ausschließlich* um die Anwendungen handelt.

PaaS bietet IT-Abteilungen bedeutende Vorteile. Der wichtigste Vorteil sind die Kosteneinsparungen aufgrund der reduzierten oder gänzlich entfallenden Wartung von Systemsoftware und anderen Routineaufgaben. Zur optimalen Nutzung des Modells erfordert PaaS in der Regel jedoch eine Neugestaltung der Anwendung.

Software as a Service (SaaS)

Beim Software-as-a-Service-Modell (SaaS – ausgesprochen „sass“) mieten Sie eine Anwendung einfach bei einem Anbieter, z. B. Microsoft Office 365 für E-Mail und Produktivität. Hierbei handelt es sich um die kostengünstigste Option, da die IT-Abteilung in der Regel nur für die Bereitstellung von Nutzern und Daten sowie, möglicherweise, für die Integration der Anwendung mit Single Sign-On (SSO) zuständig ist. SaaS-Anwendungen werden meist für Funktionen verwendet, die nicht als unternehmensverändernd erachtet werden, da benutzerdefinierte Anwendungen Geschäftsmodelle und Regeln verschlüsseln.

Wie wir in Kapitel 6 weiter ausführen werden, sollten Sie bei der Wahl der Methode für den Umstieg auf die Cloud immer nach Möglichkeiten zur Verwendung von SaaS-basierten Anwendungen suchen. In der Regel bieten diese Anwendungen den höchsten Return on Investment (ROI).

Container

Container – die im „As-a-Service“-Spektrum zwischen IaaS und PaaS einzuordnen sind – bieten die Möglichkeit, eine einzige Instanz eines Betriebssystems für mehrere Anwendungen gemeinsam zu nutzen (siehe Abbildung 2-3). Die Verwendung von Containern garantiert eine angemessene Isolierung und Sicherheit und verhindert, dass Anwendungen sich gegenseitig „im Weg stehen“. Da zum Starten einer containerisierten Anwendung in der Regel nicht eine ganze VM mit einem Betriebssystem geladen und initialisiert werden muss, kann der Start über Container sehr schnell und das Herauf- und Herunterskalieren somit sehr performant sein.

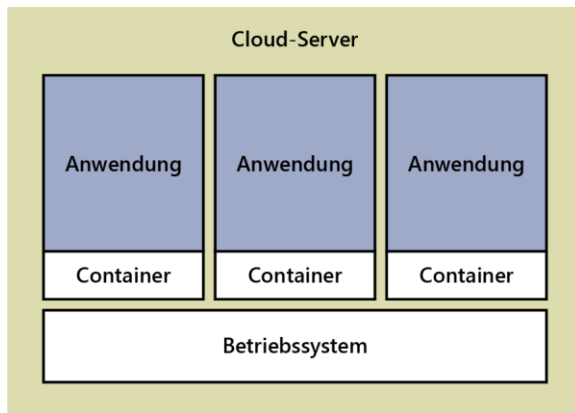


Abbildung 2-3: Containerarchitektur

Container bieten viele Vorteile. Oft ist es möglich, eine Anwendung mit wenigen oder nur kleinen Änderungen zur Ausführung innerhalb eines Containers zu verpacken. Nach der Erstellung von Containern ist es aus Gründen der Skalierbarkeit oder Resilienz oft sinnvoll, mehrere Kopien bereitzustellen. Eine verwandte Technologie, die *Orchestrierung*, kann dabei helfen, die Bereitstellung einer großen Anzahl von Kopien vieler verschiedener Anwendungen oder Komponenten auf einem Cluster von Servern zu automatisieren. All diese Aspekte und auch die Einschränkungen werden wir in Kapitel 10 detaillierter erörtern.

„As-a-Service“-Modelle im Vergleich

Abbildung 2-4 zeigt einen Vergleich zwischen den verschiedenen „As-a-Service“-Technologien und On-Premises-Computing. Die blau dargestellten Elemente sind die Komponenten oder Softwareanwendungen, für deren Wartung das Unternehmen (Sie) verantwortlich sind. Die Elemente in Orange liegen in der Verantwortung des Cloud-Anbieters.

Wie Sie sehen, ist bei einem On-Premises-Rechenzentrum das Unternehmen für alles verantwortlich, angefangen beim Rechenzentrumsbetrieb über die Einrichtungen, Strom und Klimaanlage bis hin zu den Anwendungen. Im Laufe der Migration zur Cloud werden immer mehr dieser Ausgaben vom Cloud-Anbieter getragen.

Anwendungen	Anwendungen	Anwendungen	Anwendungen
Datenbanken	Datenbanken	Datenbanken	Datenbanken
Sicherheit	Sicherheit	Sicherheit	Sicherheit
Betriebssysteme	Betriebssysteme	Betriebssysteme	Betriebssysteme
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Server	Server	Server	Server
Speicher	Speicher	Speicher	Speicher
Vernetzung	Vernetzung	Vernetzung	Vernetzung
Rechenzentrum	Rechenzentrum	Rechenzentrum	Rechenzentrum
On-Premises Rechenzentrum	Cloud IaaS	Cloud PaaS	Cloud SaaS

Abbildung 2-4: „As-a-Service“-Modelle im Vergleich

Kapitel 3

Der Weg zur Cloud: Planung

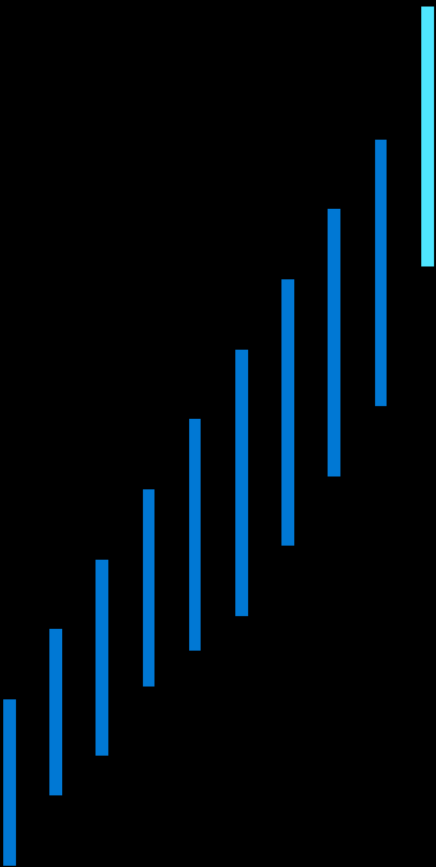
Stellen Sie sich vor, Sie könnten in allen Unternehmensbereichen und -anwendungen Ihres gesamten Portfolios für Effizienz und Innovation sorgen. Stellen Sie sich vor, Sie könnten die Cloud mit all ihren Ressourcen und Funktionen nutzen, um den Effekt „Das Ganze ist mehr als die Summe der Teile“ zu erzielen. Mit einer guten Planung ist das möglich. In diesem Kapitel sehen wir uns an, was der Umstieg Ihres Unternehmens auf die Cloud bedeutet.

Bei jeder Transformation ist es wichtig, das Ziel zu kennen und zu wissen, wie die Wegpunkte entlang der Reise aussehen werden. Für jede Anwendung gibt es verschiedene potenzielle Ziele, und die Bereitstellung der IT-Cloud wird mehrere davon kombinieren.

Modernisierungsmöglichkeiten nutzen

Bevor wir fortfahren, möchten wir anmerken, dass die Cloud eine Möglichkeit bietet, die IT-Infrastruktur und ihre Modernisierung als Ganzes zu betrachten. Wie Sie sehen werden, wird bei der Cloud-Migration im großen Maßstab jede Anwendung geprüft und ermittelt, wie sie in dieser neuen Umgebung – der Cloud – gestaltet werden soll. Sind weitere Investitionen in bestimmte Anwendungen gerechtfertigt? Sollten sie außer Betrieb genommen werden?

Viele Unternehmen verwenden ihre Anwendungen schon viel zu lange ohne Wartungs- oder Stilllegungsplan. Aus Furcht vor der Komplexität und einem Mangel an Dokumentation, Ressourcen, Quellcode oder anderen Gründen bleiben Anwendungen daher unberührt.



Sogar bei On-Premises-Anwendungen kann durch die Modernisierung Zeit und Geld gespart werden. Vor einigen Jahren zeigte eine interne Microsoft-Studie, dass die Anzahl von Problembereichten („Tickets“) und der Zeitaufwand für die Behebung dieser Probleme mit dem Alter der Anwendung und der Systemsoftware zunehmen. (Seit dieser Analyse wird verstärkt darauf geachtet, dass alle Anwendungen der aktuellen Version des Betriebssystems und anderer Systemsoftware wie Datenbanken entsprechen.)

Die Chancen, die die Cloud IT-Abteilungen bietet, sind bahnbrechend: Sie können die gesamte Infrastruktur neu bewerten und insbesondere Anwendungen bewerten und modernisieren. Allein diese Aktivität kann zu einer hervorragenden Rendite führen und den Umsatz fördern.

Die fünf Pfeiler der Modernisierung

Um unsere Bemühungen für vorhandene Anwendungen zu konzentrieren, beginnen wir mit den einfachsten Möglichkeiten zur Modernisierung:² Außer Betrieb nehmen, ersetzen, beibehalten und verpacken, neu hosten und neu gestalten. Diese Ontologie wurde ursprünglich von Gartner im Jahr 2011 formuliert und von uns im Laufe der Jahre auf Grundlage unserer Erfahrungen erweitert.

Wahrscheinlich reicht ein einzelner Ansatz für alle älteren Anwendungen eines Unternehmens nicht aus, sodass wie in Abbildung 3-1 dargestellt eine Kombination aus verschiedenen Ansätzen erforderlich wird, die auf dem Wert basiert, den eine Anwendung im Vergleich zu den Kosten eines anderen Ansatzes bietet. Da diese Ansätze stark von der jeweiligen Situation, Anwendung und Art der Kosten abhängen, gibt es keine Universallösung.



Abbildung 3-1: Verschiedene Modernisierungsinitiativen

Außer Betrieb nehmen Wenn eine ältere Anwendung im Verhältnis zu ihren Kosten wenig Nutzen und Wert bietet, sollte das Unternehmen natürlich erwägen, sie außer Betrieb zu nehmen. Wenn nur wenige Personen eine Anwendung relativ zu ihren Kosten verwenden, muss das Unternehmen eine Kosten-Nutzen-Analyse erstellen, um zu ermitteln, ob die Kosten tragbar sind. Manche Funktionen von älteren Systemen können auch in eine konsolidierte moderne Cloud-Anwendung integriert werden, sodass einige Anwendungen außer Betrieb genommen werden, während andere ersetzt und modernisiert werden.

- **Ersetzen** Häufig bietet eine ältere Anwendung zwar noch einen gewissen Wert, doch eine Ersatzlösung mit geringeren Gesamtbetriebskosten ist verfügbar. Viele veraltete Anwendungen wurden ursprünglich entwickelt, da es zu diesem Zeitpunkt keine Alternative gab. Möglicherweise

² Basierend auf „Gartner Identifies Five Ways to Migrate Applications to the Cloud“, Gartner Inc, 2011. <http://www.gartner.com/newsroom/id/1684114>

gibt es mittlerweile eine moderne, direkt verfügbare Anwendung, die sich besser für die Ausführung in der Cloud eignet (am kostengünstigsten wäre hier eine SaaS-Anwendung) und die ältere Anwendung ersetzen kann. Wenn eine veraltete Anwendung durch eine umfassendere moderne Lösung ersetzt wird, können möglicherweise auch die Funktionen verschiedener älterer Anwendungen konsolidiert und mehrere Anwendungen durch ein einziges System ersetzt werden.

- **Beibehalten, verpacken und erweitern** Wenn eine ältere Anwendung von großem Nutzen und Wert ist und keine hohen Gesamtbetriebskosten verursacht, kann sie beibehalten werden, erhält aber eine moderne „Verpackung“, um Mehrwert und zusätzliche Vorteile zu erschließen. Ein solcher Ansatz sieht beispielsweise wie folgt aus:
 - Mit API-Verwaltungstools (z. B. Microsoft Azure API Management) wird eine API hinzugefügt, sodass autorisierte externe Anwendungen die Funktion der Anwendung übernehmen können.

Eine ältere Anwendung wird um externe Tools erweitert, z. B. durch einen C#-Wrapper um ältere Anwendungen oder durch Verfügbarmachen der zugehörigen Daten mittels Extrahieren, Transformieren und Laden (ETL) oder anderer Methoden, und mit anderen Softwarekomponenten wie Analytics-Anwendungen, Machine Learning oder mobilem Zugriff verbunden.

- **Neu hosten** Wenn eine ältere Anwendung großen Nutzen und Wert bietet, ihre Ausführung aber kostspielig ist, könnte es sinnvoll sein, sie neu zu hosten. Wenn Sie neu hosten, behalten Sie dieselben Funktionen und profitieren zudem von der einfacheren Verwaltung und den geringeren Kosten für die Ausführung. Dieser Ansatz wird auch als „Lift und Shift“ bezeichnet. Beim Rehosting befindet sich die ältere Anwendung möglicherweise auf einer lokalen virtuellen Maschine (VM) oder auf lokaler Hardware. Manche VMs können unter Umständen durch einfache Migration verschoben werden. Die VMs auf lokaler Hardware können vielleicht mit einer Migration von physisch zu virtuell konvertiert werden und dann die VM in der Cloud hosten. Manche VMs, insbesondere ältere, können nicht so einfach zur Cloud migriert werden. In diesen Fällen sollten Sie in Betracht ziehen, die Anwendung neu zu gestalten und in der Cloud zu entwickeln.
- **Neu gestalten** Wenn eine ältere Anwendung großen Nutzen und Wert bietet, aber nicht einfach migriert werden kann, ist es möglicherweise am besten, sie neu zu gestalten und in der Cloud neu zu entwickeln. Beim Neugestalten wird die Anwendung in der Cloud mit moderner Technologie, einer neuen Architektur und Best Practices neu entwickelt. In der Regel sorgt sie so für einen höheren Geschäftswert und trägt durch wichtige Funktionen zur besseren Abgrenzung von der Konkurrenz bei. Beim Neugestalten einer Anwendung muss möglicherweise die Hauptlogik mit einer modernen Entwicklungssprache und Tools neu geschrieben und serviceorientiert gestaltet werden. Das Neugestalten einer Anwendung kann durch VMs in der Cloud erleichtert werden. Die Instanziierung dauert nur wenige Minuten.

Wie Sie noch sehen werden, bietet die Cloud zahlreiche Möglichkeiten zur Neugestaltung von Anwendungen. Beispielsweise kann es sinnvoll sein, „Auslagerungsmodelle“ in Erwägung zu ziehen. Bei einem solchen Modell werden bei zunehmender Belastung der On-Premises-Anwendung neue Instanzen in der Cloud erstellt, die den vorübergehenden Mehrbedarf auffangen. Ein weiteres gängiges Verfahren ist, häufig genutzte („heiße“) Daten lokal zu speichern und ältere, nur unregelmäßig genutzte („kalte“) Daten in günstigere Cloudspeicher auszulagern. Mit diesen Strategien werden wir uns an späterer Stelle im Buch befassen.

Es gibt eine Reihe von Möglichkeiten, die Sie bei der Entwicklung Ihrer Strategien für ältere Anwendungen bedenken sollten. Eine dieser Möglichkeiten besteht darin, die Anwendungen wie in Abbildung 3-2 dargestellt basierend auf der Workload zu beurteilen.

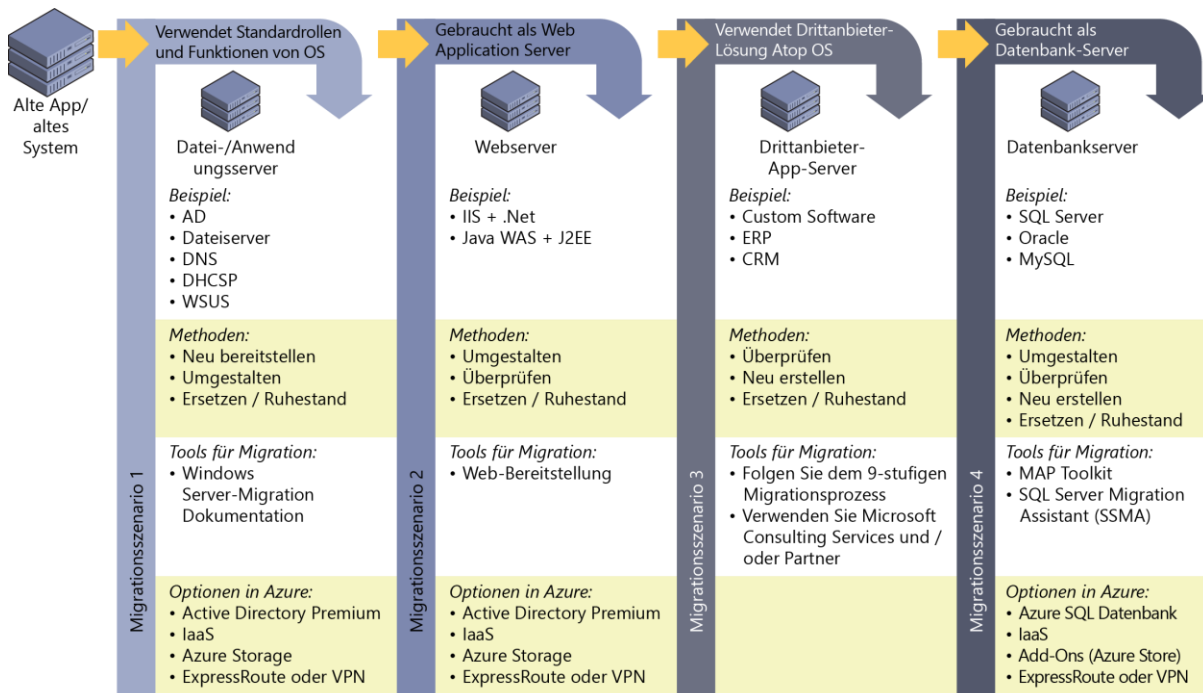


Abbildung 3-2: Strategien für ältere Anwendungen

Wie die Abbildung zeigt, können Sie ältere Software aktualisieren, indem Sie sie auf modernen Plattformen neu hosten, oder zur Cloud migrieren, um von weiteren Vorteilen zu profitieren. In den folgenden Kapiteln werden wir uns noch ausführlicher mit den einzelnen Technologien, ihrer Migration und ihrer Verwendung befassen.

Die drei Phasen der Cloud-Migration

Beim Planen der Migration zur Cloud gibt es mehrere Möglichkeiten. Unserer Erfahrung nach lässt sie sich in drei Phasen einteilen: *Experimentieren*, *Migration* und *Transformation*. Eine Anmerkung, bevor wir beginnen: In fast allen Fällen, die wir gesehen haben, finden diese drei Phasen nicht nacheinander, sondern vielmehr gleichzeitig statt. Die Gründe dafür sind im Moment vielleicht nicht offensichtlich. Oft kommt es jedoch vor, dass eine Gruppe im Unternehmen noch mit bestimmten Anwendungen in der Cloud experimentiert, während andere die Umstellung auf, beispielsweise, eine SaaS-Anwendung bereits vollzogen haben. Sie müssen also nicht den Abschluss der Experimentierphase abwarten, bevor Sie etwas Neues ausprobieren.

Experimentieren

In der Experimentierphase finden zwei Prozesse statt. Im ersten erstellen die Techniker und andere die ersten Cloud-Anwendungen der IT-Abteilung mit dem Ziel, alles über die Cloud zu erfahren: Entwicklung, Test, Bereitstellung, Überwachung und Wartung einer Cloud-Anwendung. Unternehmen und IT-Abteilungen stellen sich vor, was machbar ist. Sie entwickeln neue Lösungen, um aufzuzeigen, wie der Status quo verbessert werden kann, und überlegen, wie eine Anwendung oder ein Dienst erneuert, erweitert oder flexibler und besser gestaltet werden kann.

Migration

In der Migrationsphase – der anspruchsvollsten der drei Phasen – wird das IT-Portfolio in irgendeiner Form in die Cloud verschoben. Dies erfordert eine enge Zusammenarbeit zwischen verschiedenen Unternehmensbereichen: Techniker, Betriebsteam, Geschäftsführung, Sponsoren, Sicherheitsexperten, Compliance-Team, Rechtsabteilung und Personalwesen. In diesem Buch werden sämtliche Aspekte der Migration sehr ausführlich erläutert.

Transformation

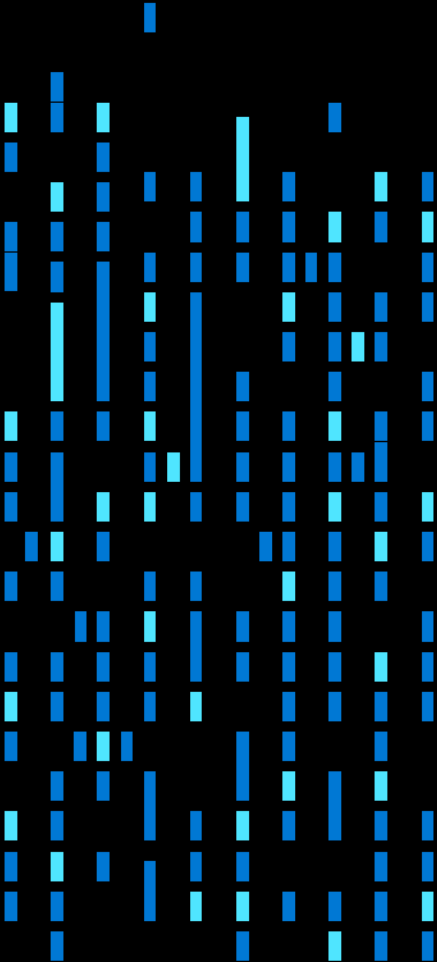
In der Transformationsphase (die sich häufig mit der Migrationsphase überschneidet) werden ausgewählte Anwendungen neu gestaltet, um – mit dem Platform-as-a-Service-Modell – maximalen Nutzen aus der Cloud zu ziehen und somit von höherer Skalierbarkeit, besserer Integration in andere Cloud-Dienste sowie zahlreichen weiteren Vorteilen zu profitieren.

Die nativen Anwendungen der Cloud können dann Cloud-Dienste wie Machine Learning, Big Data, Streaming-Analytics usw. nutzen, sodass sie deutlich mehr Funktionen und Features bieten als je zuvor.

In den folgenden Kapiteln sehen wir uns die einzelnen Phasen genauer an.

Kapitel 4

Experimentieren



Es gibt immer eine erste Cloud-Anwendung. In jeder IT-Organisation wird einmal ein mutiger Mitarbeiter eine vorhandene Anwendung in die Cloud verschieben oder dort eine neue Anwendung erstellen. Dadurch erhält er ein umfassendes Verständnis vom Entwickeln, Testen, Bereitstellen und Warten einer Cloud-Anwendung.

Die erste Cloud-Anwendung von Microsoft IT

Microsoft IT entwickelte 2010 seine erste Cloud-Anwendung. Es handelte sich um eine Auktionsanwendung für Mitarbeiter, die einmal pro Jahr im Rahmen der Charity-Kampagne von Microsoft zum Einsatz kam (siehe Abbildung 4-1). Mitarbeiter können Dinge spenden (von Mentoring-Einheiten über Kochkurse und Software bis zur Nutzung eines Fahrzeugs der Geschäftsführung), die andere kaufen. Der Erlös geht an Wohltätigkeitsorganisationen. Die Auktion läuft einen Monat lang, in der Regel im Oktober.

Warum wählten wir diese Lösung als erste Cloud-Anwendung? Nun, dafür gab es mehrere Gründe: Erstens, war es keine geschäftskritische Anwendung. Daher würden Nachrichten über Probleme mit der Anwendung weder den Finanzen noch dem Ruf des Unternehmens schaden noch auf irgendeiner Titelseite erscheinen.

Zweitens konnten wir die Skalierbarkeit von Microsoft Azure in Aktion erleben. Gegen Ende Oktober nahm der Traffic der Anwendung kontinuierlich zu und erreichte seinen Höchststand an den letzten Tagen der Auktion.

Es war eine relativ simple Anwendung, deren Bereitstellung in der Cloud kein gleichzeitiges Upgrade von anderen Anwendungen erforderte.

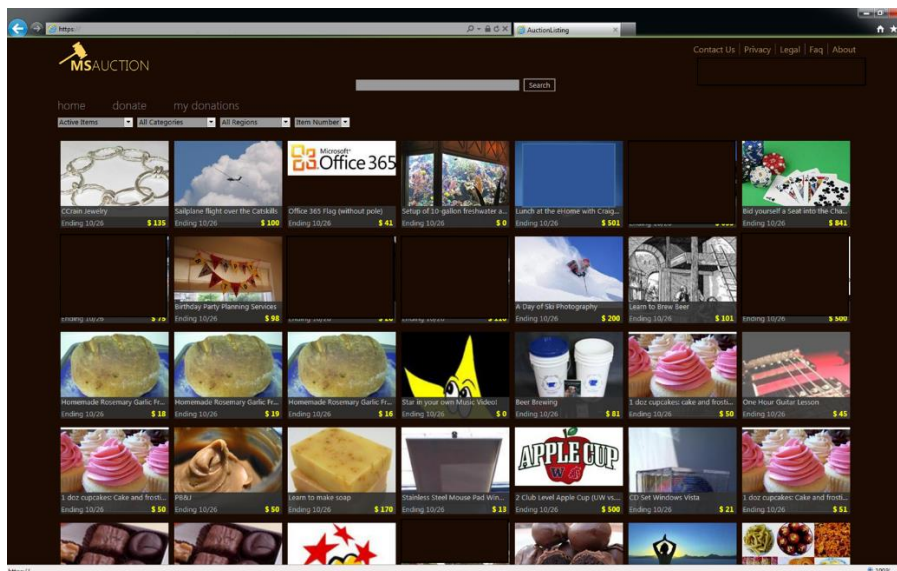


Abbildung 4-1: Interne Auktionsanwendung von Microsoft, ca. 2010³

Die Anwendung war äußerst erfolgreich, und die Auktion erfüllte ihre Ziele (die Mitarbeiter von Microsoft haben im Laufe der Jahre mehr als eine Milliarde Dollar für wohltätige Zwecke gesammelt). Microsoft IT sammelte Erfahrung in der Cloud-Entwicklung und -Bereitstellung und konnte wertvolles Wissen zusammentragen, das wir in den folgenden Phasen unserer eigenen Umstellung auf die Cloud erfolgreich einsetzten. Wir erlebten, wie einfach die Anwendung skaliert werden konnte, um dem steigenden Bedarf im Laufe des Monats gerecht zu werden. Am Ende der Auktion konnten wir die Anwendung abschalten und mussten somit keine Ressourcen für die Ausführung mehr bezahlen – hätten wir die Anwendung in unserem Rechenzentrum ausgeführt, wären Kosten für Server, Mitarbeiter usw. angefallen. Dieses erste Experiment war in jeder Hinsicht ein voller Erfolg.

In diesem Zeitraum führten wir viele weitere Experimente durch, testeten neue Ansätze, neue Features usw. Wir erfuhren, dass die Einführung einer „Kultur des Experimentierens“ uns zugute kam, da wir ständig Neues ausprobieren und Innovation vorantreiben konnten.

Wenn Sie noch am Anfang stehen, sollten Sie Ihre ersten Anwendungen vielleicht dazu nutzen, die Möglichkeiten der Cloud gründlich zu erkunden: Verwenden Sie Telemetrie, um den Betrieb der Anwendungen zu überwachen. Sammeln Sie die Daten, und analysieren Sie sie mithilfe der Big Data- und Analytics-Funktionen, die Ihnen in der Cloud zur Verfügung stehen. Entwickeln Sie ein Dashboard, oder verwenden Sie Machine Learning, um das Benutzerverhalten vorherzusagen. All dies sind hervorragende Möglichkeiten, um Ihre Mitarbeiter mit Cloud-Diensten vertraut zu machen. Diese Mitarbeiter bilden dann den Kern Ihres Cloud-Kompetenzzentrums und teilen ihre Erfahrungen mit anderen Mitgliedern Ihres Teams.

³ Mentoring, Tutorienübungen und persönliche Gespräche mit Führungskräften stehen immer zur Auktion. Im Sinne des Datenschutzes haben wir die Gesichter der Personen vom Screenshot entfernt, die diese Sitzungen anbieten. Daher sind einige Quadrate leer.

Schatten-IT und die Kultur des Experimentierens

IT-Abteilungen befinden sich häufig in einer Welt der Widersprüche. Einerseits müssen sie den Betrieb am Laufen halten, indem sie Server und Netzwerke pflegen, Berichte rechtzeitig abliefern und sicherstellen, dass die Systeme, Daten und ihre unterstützenden Prozesse den gesetzlichen Vorschriften entsprechen, beispielsweise dem Sarbanes-Oxley-Gesetz, dem HIPAA-Gesetz (Health Information Portability and Accountability Act), dem PCI DSS (Payment Card Industry Data Security Standard) und zahlreichen anderen Regularien. Diese Anforderungen sind sehr streng – und notwendig. (Das Thema Compliance wird in Kapitel 9 ausführlicher behandelt.)

Andererseits sind sich die IT und ihre Geschäftspartner der Bedeutung – oder vielmehr der absoluten *Notwendigkeit* – von Innovation bewusst: neue Programme und neue Anwendungen zu unterstützen, die neue Geschäftschancen eröffnen, einen besseren Kundenservice ermöglichen usw. Zudem schränken die IT-Betriebskosten, die teilweise 70-80 % des Gesamtbudgets ausmachen, die IT häufig bei der Investition in neue Programme und Innovationen ein.

In vielen Fällen (in jedem Unternehmen, das wir kennen) werden gelegentlich Anwendungen außerhalb der IT-Abteilung erstellt und bereitgestellt, um auf dringende Geschäftsanforderungen zu reagieren. Diese inoffiziellen Anwendungen werden häufig als „Schatten-IT“ bezeichnet. Statt die bei der Erstellung neuer IT-Anwendungen üblichen Phasen von Budgetprüfung, Bedarfsanalysen, Entwicklung und Bereitstellung zu durchlaufen, erstellt beispielsweise eine Marketingabteilung für eine neue Kampagne einfach selbst eine Website.

Da die Komponente der Kapitalinvestitionen (d. h. Server, Speicher und Netzwerk) der Anwendungsentwicklung entfällt, erleichtert die Cloud schnelle Innovationen dieser Art erheblich. Zum Schreiben der Anwendung sind lediglich ein paar Programmierer erforderlich – und eine Kreditkarte.⁴

IT-Führungskräfte sollten realisieren, dass diese Art der Innovation und Experimente unumgänglich und in vielen Fällen erstrebenswert ist. Da sich das Geschäftsklima ständig ändert, müssen Unternehmen und IT-Organisationen schnelle Experimente und Innovationen fördern.

Selbstverständlich wird es wichtig sein, Unternehmen die Bedeutung und Konsequenzen von regulatorischen Fragen und Verstößen gegen Vorschriften aufzuzeigen. IT-Abteilungen können dazu beitragen, indem sie kontrollierten, verwalteten Zugriff auf kritische Daten wie Kundeninformationen bereitstellen, anstatt diesen Unternehmen das eigenmächtige Erfassen und Verändern von Daten zu erlauben.

Sobald ein Unternehmen mit diesem Prozess der Planung beginnt und die Kultur des Experimentierens schafft, wird es mit den Fakten konfrontiert: In Zeiten der Cloud müssen wir experimentieren, schnell scheitern und schnell daraus lernen. Experimente sind wichtig, um schnell aus Erfolgen und Misserfolgen zu lernen. Diese Lernprozesse schaffen die Grundlagen, um das enorme Innovations- und Wertschöpfungspotenzial der Cloud nutzen zu können.

Prinzipien einer Kultur des Experimentierens

Für die traditionelle IT-Organisation mag die Kultur des Experimentierens befremdlich erscheinen, da ihr Hauptaugenmerk sehr oft der sorgfältig kontrollierten Entwicklung und Risikominderung gilt. Das Fördern von Experimenten wird den Prozess der Einführung der Cloud jedoch erheblich verbessern.

Die Prinzipien, die wir angewendet haben, lauten wie folgt: *schnell handeln*, *Grenzen durchbrechen*, *datengestützte Entscheidungen* treffen, *vereinfachen* und zu guter Letzt *kommunizieren*, um erfolgreich zu sein. Tabelle 4-1 enthält einen Übersicht über diese Prinzipien sowie eine detaillierte Beschreibung jedes Prinzips.

⁴ Die Eliminierung derartiger Kapitalausgaben hat die Geschwindigkeit, mit der Startups in die Höhe schießen, enorm gesteigert.

Tabelle 4-1: Prinzipien der Cloudmigration

Schnell handeln	Grenzen durchbrechen	Datengestützte Entscheidungen treffen	Vereinfachen	Kommunizieren, um Erfolg zu haben
Schnell scheitern, schnell daraus lernen Vieles probieren, das Beste nehmen	Neue Anwendungen und Funktionen für PaaS/SaaS entwickeln Veraltete Apps für PaaS/SaaS umgestalten Plan entwickeln, um von der Cloud zu profitieren „Erfahrung“ bedenken	Kosten verwalten Mit Telemetrie Einblick in betriebliche Effizienz erhalten Blockaden kennen Plan verwalten	Veraltete Anwendungen außer Betrieb nehmen, wo möglich Aggressiv dimensionieren Inaktive Server wöchentlich überprüfen Configuration Management Database (CMDB)-Daten bereinigen	Auswirkungen auf Kunden und Beteiligte kommunizieren – Transparenz ist unabdingbar Erkenntnisse und Best Practices austauschen

- **Schnell handeln** Dieses Prinzip veranschaulicht den Geist der Experimentierphase. Für manche stellt sie eine neue Denkweise für die IT dar, da mit der Cloud neue Projekte schnell mit wenigen Klicks erstellt werden können. IT-Abteilungen müssen nicht mehr umständlich planen, Platz im Rechenzentrum zuweisen, Ausstattung kaufen usw. Wir bezeichnen diesen Ansatz als *vieles probieren, das Beste nehmen*, da die Cloud IT-Abteilungen die Auswahl der besten von vielen Lösungen deutlich vereinfacht.
- **Grenzen durchbrechen** Dieses Prinzip besagt, dass die IT sich nicht einfach den neuen Paradigmen der Cloud anpassen, sondern diese nutzen und schnell neue Architekturen und Prozesse einführen sollte, um das neue Potenzial auszuschöpfen.
- **Datengestützte Entscheidungen treffen** Dieses Prinzip bedeutet, Zahlen sorgfältig zu dokumentieren und zu bewerten – die Kosteneffizienz der Cloud aus Finanzgründen, die Systemtelemetrie aus Gründen der technischen Effizienz usw. Die sorgfältige Prüfung der Daten ermöglicht es Ihnen, fundierte Entscheidungen darüber zu treffen, welche Anwendungen den meisten Umsatz generieren, welche priorisiert werden sollten, welche in der Cloud gut funktionieren und wo potenzielle Problembereiche liegen.
- **Vereinfachen** Bei diesem Prinzip geht es in erster Linie um die Außerbetriebnahme, korrekte Dimensionierung und Konsolidierung möglichst vieler Dienste und Anwendungen. Unregelmäßig oder selten genutzte Anwendungen verursachen einer IT-Organisation häufig hohe Kosten und sorgen kaum für Umsatz. Wenn Sie diese Anwendungen außer Betrieb nehmen und mit Anwendungen mit ähnlicher Funktion konsolidieren, können Sie in Bereichen wie Hardware, Systemsoftwarelizenzen und Wartung Einsparungen erzielen. Legen Sie auf der CPU-, Netzwerk- und Datenbankauslastung basierende Kennzahlen für inaktive Anwendungen fest. Eine Anwendung mit durchschnittlich 2 % CPU-Auslastung und wenig authentifizierten Benutzern ist beispielsweise möglicherweise einfach inaktiv.

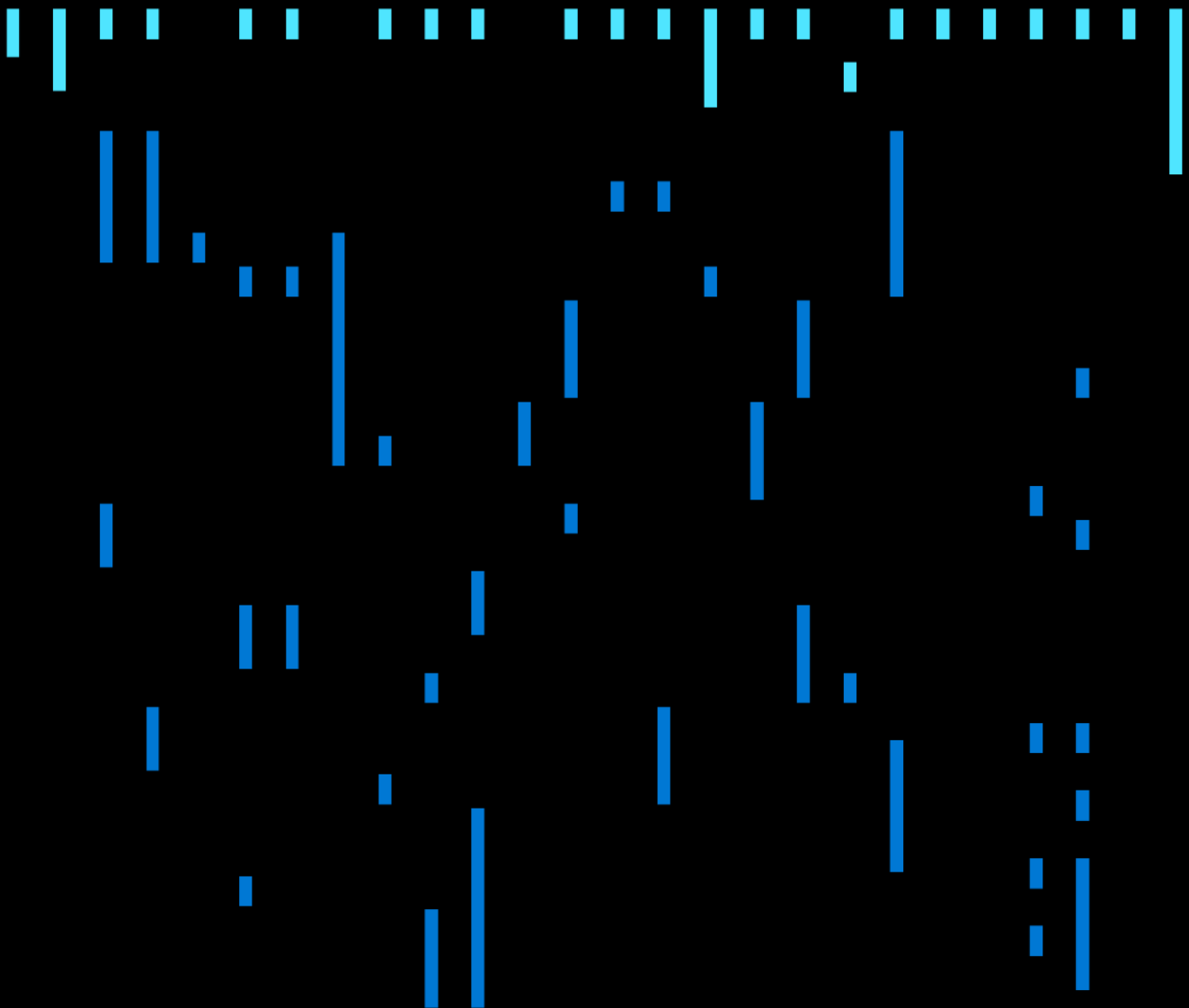
- **Kommunizieren, um Erfolg zu haben** Dieses Prinzip ist von größter Bedeutung, da es langfristigen Erfolg und nicht nur die Migration einer einzigen Anwendung oder eines Diensts garantiert. Erstellen Sie einen klaren und kontinuierlichen Kommunikationskanal für alle Beteiligten, um Erfolg und Auswirkungen zu veranschaulichen sowie Fehler und die daraus gelernten Lektionen zu verstehen. Wichtige Beteiligte bleiben motiviert und bringen sich weiter aktiv ein, wenn sie spüren, dass ihre Beteiligung erforderlich ist, um nicht nur einen einmaligen, sondern kontinuierlichen Erfolg sicherzustellen.

Ein gut durchdachter Ansatz im Hinblick auf Experimente kann äußerst lohnend sein. Experimentieren bedeutet keineswegs, dass sämtliche Kontrollen entfallen. Vielmehr sollten IT-Führungskräfte „Sandboxes“ für die Durchführung von Experimenten einrichten. Sinnvoll ist es beispielsweise, Experimente auf nicht geschäftskritische Unternehmensanwendungen oder -prozesse zu beschränken, den Zugriff auf sensible Daten wie personenbezogene Informationen (PII) zu unterbinden usw.

Aus Experimenten lässt sich viel lernen. Die gesammelten Erfahrungen und Erkenntnisse rüsten uns für die Migrationsphase, mit der wir uns in Teil II befassen.

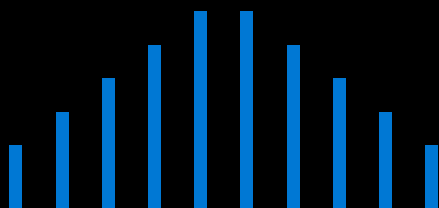
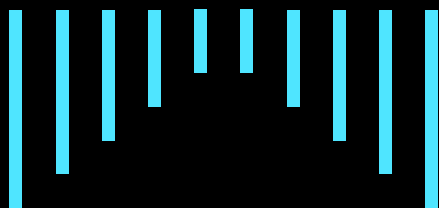
Teil II

Umstellung der IT auf die Cloud



Kapitel 5

Entwicklung der Voraussetzungen



Früher oder später wird offensichtlich, dass es aus verschiedenen Perspektiven sinnvoll ist, viele IT-Anwendungen – vermutlich den Großteil des IT-Portfolios – in der Cloud auszuführen. Wie wir in Teil I erörtert haben, bietet die Ausführung in der Cloud eine Reihe von Vorteilen, darunter Kosteneinsparungen, Flexibilität und Innovationsmöglichkeiten. Die Argumente, die für die Cloud sprechen, sind überzeugend. Die Migrationsphase betrifft in der Regel jedoch viel mehr Anwendungen und Personen, und sie wirkt sich möglicherweise auf deutlich mehr IT-Kunden aus als alle anderen Phasen.

Für die IT-Abteilung eines großen Unternehmens kann die Verwaltung von Hunderten oder Tausenden Anwendungen auf bis zu Zehntausenden virtuellen Maschinen (VMs) eine große Herausforderung darstellen. Welche werden zuerst verschoben? Wie sollen Prioritäten gesetzt werden? Wie wirkt sich der Betrieb in der Cloud auf die Einhaltung von Vorschriften, Datensicherheit und Unternehmensprozesse aus? Welche Auswirkungen ergeben sich für Organisationsrollen, Schulung und Änderungsmanagement? Und nicht zuletzt stellt sich die Frage: Wie soll das alles im laufenden Betrieb bewältigt werden?

Wo sollen wir anfangen?

In Teil II beschreiben wir, wie Strategien und Ziele für die Cloud-Migration festgelegt werden, welche Rollen die verschiedenen Organisationen im Unternehmen spielen, welche Prioritäten bei der Anwendungsmigration gesetzt werden sollten und wie die IT-Governance um die Cloud erweitert wird.

Festlegen von Strategien und Zielen

Bei jeder Reise werden Ziel, Strecke und Ankunftszeitpunkt geplant. Bei einer Migration zur Cloud ist das nicht anders. IT-Führungskräfte und die Unternehmensleitung sollten sich mit allen Aspekten der Cloud vertraut machen und sich über die vielen Optionen und Ansätze informieren – die Zeit ist gut investiert.

Bei Microsoft IT begann die Reise wie in vielen Unternehmen mit der Bildung eines Cloud-Strategieteams, das (in unserem Fall) vom CTO geleitet wird und aus Mitgliedern des Unternehmensarchitekturteams, des IT-Finanzteams, den erfahrensten Technologien aus verschiedensten IT-Anwendungsgruppen (Personal- und Finanzwesen usw.) und Führungskräften der Infrastruktur-, Sicherheits- und Netzwerkteams besteht. Abbildung 5-1 zeigt den Aufbau des Cloud-Strategieteams.⁵

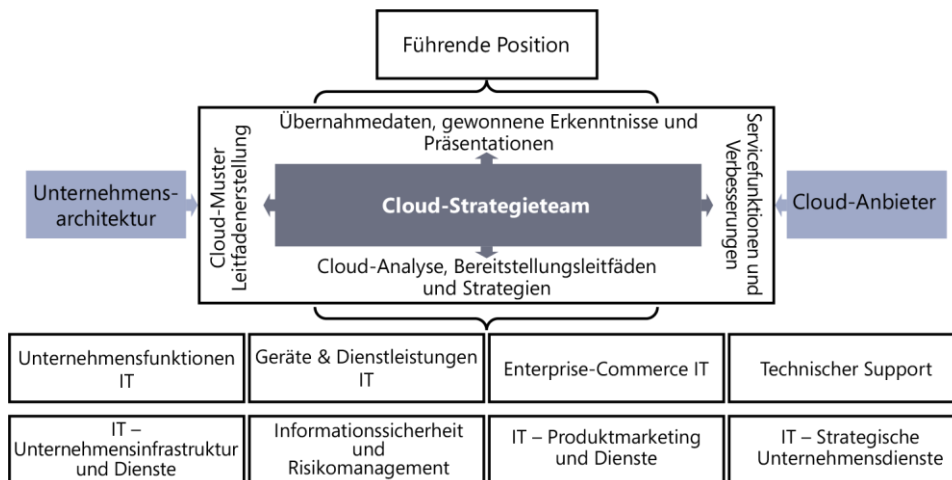


Abbildung 5-1: Das Cloud-Strategieteam von Microsoft IT

Das Cloud-Strategieteam wurde gegründet, um die zuvor beschriebenen Cloud-Analyse- und Experimentierphasen zu leiten (siehe Abbildung 5-2). Das Team entwickelte außerdem die Architekturen, Muster und Leitfäden für die Bereitstellung der neu gestalteten Anwendungen oder Dienste (oder leistete Unterstützung bei ihrer Erstellung), war für die Kommunikation mit den wichtigen Beteiligten zuständig und sorgte dafür, dass die Erfolge und durch das Programm gewonnenen Erkenntnisse an andere Teams weitergegeben wurden.

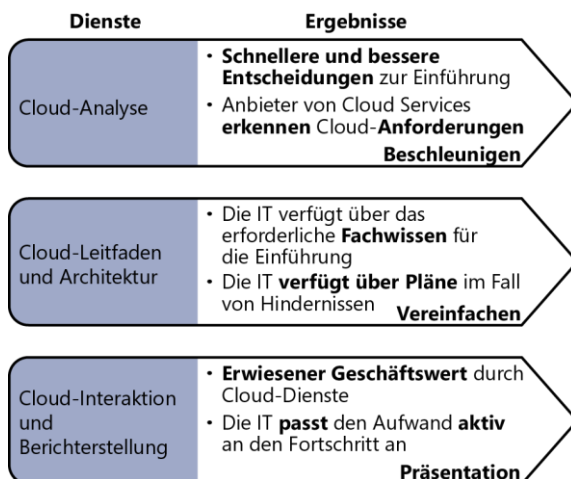


Abbildung 5-2: Aufgaben des Cloud-Strategieteams

⁵ Das „First and Best“-Team der Microsoft IT gewährleistet, dass Microsoft IT der „First and Best“-Kunde von Microsoft ist, indem alle Unternehmensprodukte in der IT getestet werden, bevor sie für die breite Öffentlichkeit freigegeben werden. Diese Vorgehensweise wird oft als „Dogfooding“ bezeichnet.

Die Bildung dieses Teams war maßgeblich, um die Beteiligten langfristig an das Projekt zu binden und ihr Engagement auf Dauer sicherzustellen. Das Team entwickelte eine Vorgehensweise für kontinuierliches Testen und Experimentieren, um die geeignete Plattform und das Ziel für jede Anwendung zu ermitteln, d. h. welche Komponenten migriert werden und welche Plattform dafür am besten geeignet ist, z. B.:

- Soll die Anwendung, sofern sie zur Cloud migriert wird, weiterhin einfach als VM für IaaS (Infrastructure as a Service) ausgeführt oder für PaaS (Platform as a Service) umgestaltet werden?
- Kann sie durch ein bereits vorhandenes SaaS-Modell (Software as a Service) ersetzt werden, um die Kosten zu senken?
- Oder sollte sie in der On-Premises-Umgebung verbleiben?

Zu den ersten Aufgaben des Teams zählte es, sich zu informieren und sicherzustellen, dass alle Teilnehmer auf demselben Wissensstand sind. Die Cloud-Technologie hat eine ganz eigene Terminologie, beispielsweise die in Kapitel 2 erläuterten Akronyme. Durch die frühzeitige Einführung einer einheitlichen Terminologie wurden künftige Besprechungen beschleunigt. Das Team machte sich zudem mit den verschiedenen Anbietern für Plattformen, Tools und Cloud-Anwendungen vertraut.

Als das Team mit dem Planen der Strategie begann, wussten die Mitglieder, dass aus verschiedenen Gründen nicht alle Dienste oder Anwendungen in die Public Cloud verlagert werden. Die Strategie von Microsoft IT beruhte daher auf dem Konzept einer *Hybrid Cloud* (siehe Abbildung 5-3). So blieben bestimmte Anwendungen zumindest für einen gewissen Zeitraum in der On-Premises-Umgebung.

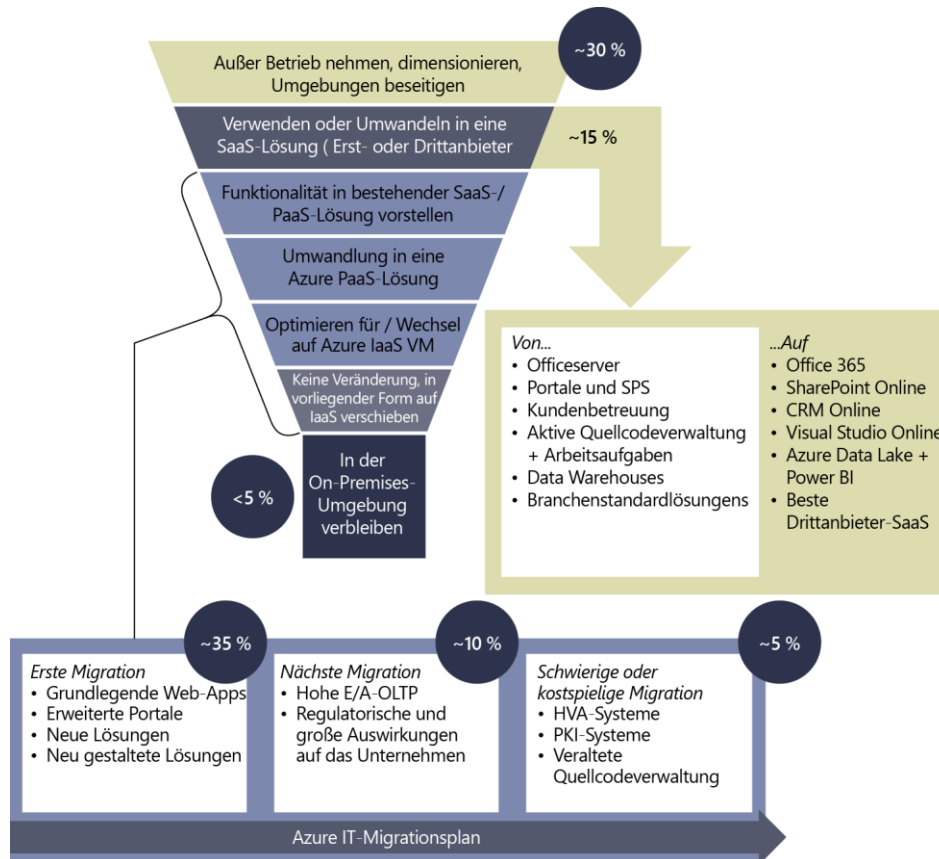


Abbildung 5-3: Hybrid Cloud-Strategie

Andererseits erkannten wir, dass die optimale Strategie aus Effizienz- und Kostengründen darin bestand, zunächst zu prüfen, ob eine Anwendung durch Konsolidierung mit einer anderen Anwendung mit ähnlicher Funktion außer Betrieb genommen oder, falls sie kaum genutzt wird, komplett entfernt werden kann.

Als Nächstes suchten wir nach Anwendungen, die auf ein SaaS-Modell umgestellt werden konnten, sodass Microsoft IT weder Hardware noch Software pflegen muss. Danach, als wir bereits in eine SaaS-Anwendung investiert hatten, aber nicht all ihre Funktionen nutzten, überprüften wir, ob wir durch die Nutzung weiterer Funktionen andere Anwendungen ersetzen können. Bestimmte Kundenanwendungen – diejenigen, bei denen eine erhebliche Neuentwicklung erforderlich war, – wurden in Microsoft Azure PaaS-Anwendungen konvertiert.

Andere Anwendungen wurden zu einer Cloud-IaaS-Umgebung migriert, was natürlich bedeutete, dass sie in der Cloud gehostet wurden, die Betriebssysteme und Datenbanken aber trotzdem weiterhin von uns gewartet werden mussten. Letztlich wurde aus verschiedenen Gründen (z. B. Legacy-Code) eine sehr geringe Anzahl von Anwendungen weiterhin lokal gehostet.

Diese Analyse werden wir in Kapitel 6 sehr ausführlich erläutern.

Das Cloud-Strategieteam erstellte ein Dokument, in dem die Ziele der Migration, die möglichen Zeitfenster, die empfohlene technische Strategie (d. h. technische Plattform und Tools) sowie erwartete Ergebnisse und Vorteile beschrieben werden. Die Empfehlungen umfassten beispielsweise Aussagen der folgenden Art:

- Der Großteil der vorhandenen Anwendungen wird zunächst auf IaaS-VMs umgestellt, da dies eine relativ schnelle Möglichkeit für den Umstieg auf die Cloud ist (keine Codeänderungen erforderlich).
- Um von Skalierbarkeit und anderen Funktionen zu profitieren, werden neue Anwendungen und größere Releases als PaaS-Anwendungen (neu)entwickelt.
- In der Übergangszeit werden lokale Anwendungen über eine eigene Verbindung (in der Regel MPLS oder WAN) mit Cloud-Anwendungen kommunizieren (in unserem Fall über ExpressRoute von Microsoft).
- Anwendungen, die nur wenig Wettbewerbsvorteile bieten (Anwendungen, die kommerzialisiert werden können), werden auf externe SaaS-Anbieter (z. B. Microsoft Office 365 für E-Mail- und Produktivitätsanwendungen) umgestellt.
- Die zu erwartenden Einsparungen betragen x % nach dem ersten Jahr und y % nach dem zweiten Jahr.
- Bestimmte Anwendungen verbleiben vorerst in der On-Premises-Umgebung (aufgrund von älteren Architekturen, der Komplexität der Integration und ähnlichen Problemen).
- Sicherheit wird durch Verschlüsselungskombinationen, Cloud-Identität in Verbindung mit lokalen Identitätsanbietern (wie Active Directory) und andere Maßnahmen sichergestellt.
- Operative Teams werden in der Cloud-Bereitstellung und Systemverwaltung in der Cloud geschult und auf lange Sicht mit einem DevOps-Modell arbeiten (dieses Modell wird an späterer Stelle erläutert).

Dokumente dieser Art können verschiedene Modelle und Optionen enthalten, die als Grundlage für Diskussionen dienen und fundierte Entscheidungen ermöglichen.

Organisatorische Aufgaben bei der Entwicklung der Strategie

Bei unseren ersten Recherchen stellte sich heraus, dass die Cloud viele Organisationen innerhalb und auch außerhalb der IT betrifft. Daher mussten wir sicherstellen, dass all diese Organisationen an der Entscheidungsfindung beteiligt werden. In diesem Abschnitt erfahren Sie, wie die folgenden Organisationen zur Cloud-Strategie beitragen:

- Unternehmensarchitektur
- Informationssicherheit und Risikomanagement
- Datenklassifizierung
- Unternehmensrisikomanagement
- Finanzen
- Operatives Geschäft
- Personalabteilung
- Anwendungsteams
- Geschäftseinheiten

Unternehmensarchitektur

Die Unternehmensarchitektur (Enterprise Architecture, EA) spielt bei der Cloud-Migration eine wichtige Rolle. Das Ziel jedes EA-Teams besteht darin, die effizienteste Nutzung der technischen Ressourcen und somit den größtmöglichen Geschäftswert sicherzustellen. Die EA ist folglich das entscheidende Bindeglied zwischen operativem Geschäft und IT.

In der Regel ist die EA für die IT-Funktionen und -Prozesse zuständig. Das EA-Team leistet Unterstützung bei der Erstellung und Implementierung von IT-Strategien, arbeitet mit dem operativen Team und Führungskräften zusammen, um die langfristigen Ziele des Unternehmens zu verstehen und für die Zukunft zu planen, und steuert verschiedene unternehmensweite Governance-Aktivitäten wie die Architekturprüfung. Aus diesen Gründen ist das EA-Team ideal dafür geeignet, die Leitung des Cloud-Strategieteam zu übernehmen.

Da das EA-Team das gesamte IT-Ökosystem betrachtet, ist es in einer guten Position, um die entsprechenden Analysen der Systemeigenschaften und Auswirkungen größerer Änderungen am Ökosystem auf die Anwendung zu erstellen. Häufig erstellt und pflegt die EA das Portfoliomanagementsystem (den Anwendungskatalog), mit dem einfacher Prioritäten beim Verlagern von Anwendungen in die Cloud gesetzt werden können (wir gehen später genauer auf diesen Prozess ein). Unternehmensarchitekten sollten prüfen, was über das Portfolio bekannt ist und welche zusätzlichen Informationen benötigt werden, z. B. ob eine Anwendung virtualisiert wurde. Das EA-Team sollte diese und andere Attribute der Wissensdatenbank hinzufügen und mit anderen IT-Teams zusammenarbeiten, um Daten zu erfassen. Weitere Beispiele für solche Metadaten werden in Kürze beschrieben.

Die Cloud-Migration eröffnet Unternehmensarchitekten zahlreiche Vorteile. Mithilfe von Modellierungstechniken wie Geschäftsfunktionsanalysen⁶ und Funktionsreifemodellen ist es während des Priorisierungsprozesses für Anwendungen meist möglich, die IT durch das Konsolidieren von Anwendungen mit ähnlicher Funktion zu *vereinfachen*. Die Konsolidierung eröffnet deutliche finanzielle Vorteile durch die Reduzierung der Computing-, Daten- und Netzwerkanforderungen sowie durch das Vereinfachen der Prozesse und Wartungsfunktionen.

Unternehmensarchitekten und insbesondere Informationsarchitekten können die Möglichkeiten, die die Migration zur Cloud eröffnet, zudem nutzen, um die von Anwendungen verwendeten Datenmodelle zu analysieren und auf ein unternehmensweites kanonisches Modell zu aktualisieren. Durch solche Aktivitäten wird die Anwendungsintegration optimiert, und semantische Diskrepanzen zwischen separaten Datenmodellen, die in einer komplexen On-Premises-Umgebung häufig manuell angepasst werden müssen, werden reduziert.

Zudem ist das EA-Team für die Entwicklung und Wartung von aktuellen und künftigen Strategien für die gesamte IT-Infrastruktur zuständig. Das IT-Team sollte in der Lage sein, die verschiedenen Migrationsphasen und aktuellen Überlegungen des Cloud-Strategieteam zusammenzufassen und zu kommunizieren.

Zur Erweiterung vorhandener Funktionen oder Bereitstellung völlig neuer Funktionen für IT-Anwendungen sollte das EA-Team zudem neue Cloud-Technologien prüfen lassen und diese Funktionen nach erfolgreicher Prüfung in die vorhandene Strategie aufnehmen. Unternehmensarchitekten müssen mit neuen Technologien experimentieren sowie der IT-Leitung und wichtigen Beteiligten ihren Geschäftswert zu kommunizieren. Erfolgreiche Prüfungen sollten zur Entwicklung und Veröffentlichung von Referenzarchitekturen führen, die Anwendungsteams wieder verwenden können.

Informationssicherheit und Risikomanagement

Jede größere Veränderung der Art, wie Sie Geschäfte tätigen, birgt gewisse Risiken. Kaum ein Aspekt der Cloud hat wurde kontroverser diskutiert als Sicherheit und Risiko. In Zeiten von Sicherheitsverstößen, landesweiten Hackerangriffen sowie wachsenden, großen Bedenken bezüglich des Datenschutzes im Internet wird Cybersicherheit zu Recht auf den Vorstandsebenen diskutiert. Staatliche Einrichtungen und Organisationen haben zur Kontrolle der Risiken Vorschriften geschaffen und Anforderungen definiert.

Informieren Sie sich zu Beginn über die Sicherheitslage der Cloud-Plattform-Anbieter. Diese umfasst z. B. die Verfügbarkeit von Malwareschutz für in der Cloud gehostete Anwendungen, Software und Tools zur Angriffserkennung, erweiterte und sichere Identitätsverwaltung, Optionen zu Verschlüsselung aktiver und ruhender Daten, Netzwerkoptionen für die lokale und externe Kommunikation, die Möglichkeit der Durchführung von Eindringtests usw. Eine „Defense in Depth“-Strategie ist erforderlich. Finden Sie heraus, in welchem Rahmen Sie zur Implementierung und Optimierung einer solchen Strategie mit Ihrem Cloud-Anbieter zusammenarbeiten können.

Zudem sollten Sie die physischen Sicherheitspraktiken des Cloud-Anbieters kennen. Sind Mitarbeiterüberprüfungen erforderlich? Wird eine biometrische Authentifizierung für den Zugriff auf das Cloud-Rechenzentrum verlangt?

⁶ Eine Modellierungstechnik, die ein Unternehmen im Hinblick auf Geschäftsfunktionen analysiert, unabhängig von Organisation oder Technologie, zuerst von Gartner entwickelt. Siehe auch <https://www.gartner.com/doc/1415831/use-business-capability-modeling-explore>. Funktionsmodelle sind nur eine mögliche Methode für die Gestaltung einer Unternehmensarchitektur. Sie können andere wie das berühmte von John Zachman entwickelte Zachman Framework verwenden oder Geschäftsprozessmodell und -notation (Business Process Model and Notation; BPMN), entweder mit oder anstelle der Funktionsgestaltung.

Da die Cloud den Zugriff auf Unternehmenscomputer rund um den Globus ermöglicht, muss das IT-Sicherheitsteam festlegen, welche Anforderungen diese Geräte für den Zugriff erfüllen müssen. Beispielsweise kann es erforderlich sein, für alle Clientgeräte die Verschlüsselung von lokalem Speicher anzufordern, beispielsweise mit Technologien wie Microsoft BitLocker. Da das Eingeben von Benutzernamen und Kennwörtern auf mobilen Geräten sehr mühsam sein kann, sollte das Team andere Authentifizierungsmöglichkeiten in Betracht ziehen, z. B. Biometrie. Sie könnten auch eine „Multi-Factor Authentication“ erwägen, bei der sowohl Benutzername und Kennwort als auch eine andere Form des Identitätsnachweises verlangt werden (z. B. eine Smartcard oder eine sekundäre Authentifizierung über ein Smartphone).

Eine ähnliche Möglichkeit in der Cloud ist, mit dem Open Authorization-Protokoll (OAuth) Authentifizierungsdaten aus verschiedenen Quellen zu akzeptieren. IT-Sicherheitsexperten müssen entscheiden, ob und welche Anwendungen die Anmeldung über (beispielsweise) Facebook- oder Google-Anmeldeinformationen akzeptieren dürfen. E-Commerce-Websites könnten von der Nutzung dieser Daten profitieren, interne Anwendungen eher nicht.

Prüfen Sie wichtige rechtliche Anforderungen, z. B. den Health Insurance Portability and Accountability Act (HIPAA), das Federal Risk and Authorization Management-Programm (FedRAMP) und GDPR, die EU-Datenschutzrichtlinie (European General Data Protection Directive, EUDPD). Für verschiedene Branchen und Geografien gelten verschiedene Vorschriften und Standards. Erfahren Sie, wie Sie einen vermuteten Verstoß aufdecken, wie Sie diesen dem Anbieter melden und welche SLA-Reaktionszeit zu erwarten ist. Vom Azure Trust Center erfahren Sie Einzelheiten zu diesen Punkten, die sich auf dieses Angebot beziehen. Die Cloud Security Alliance ist eine hervorragende unabhängige Ressource, in der Experten aus allen Branchen gemeinsam Empfehlungen für Best Practices für sicheres Computing in der Cloud erstellen.⁷

Ausführlichere Informationen zur Cloud-Sicherheit und -Governance finden Sie in Kapitel 9.

Datenklassifizierung

Überlegen Sie sich, welche Daten Ihre Anwendungen in der Cloud speichern können und wie sich diese auf Sicherheit und Risiko auswirken. Viele Unternehmen klassifizieren ihre Daten anhand ihrer Vertraulichkeit: an ein Marketingdokument ergeben sich völlig andere Sicherheitsanforderungen als z. B. ein Entwurf einer Form 10-K vor der Veröffentlichung der Gewinnerklärung.

Eine Möglichkeit ist, die Daten in verschiedene Kategorien einzuteilen, die auf der Auswirkung auf das Unternehmen im Fall einer unbefugten Freigabe basieren. Beispielsweise wäre die erste Kategorie öffentlich, zur Freigabe gedacht und somit ohne Risiko für das Unternehmen. Die nächste Kategorie hat geringe Auswirkungen auf das Unternehmen (low business impact, LBI) und umfasst Daten oder Informationen, die keine personenbezogenen Informationen oder vertraulichen Themen enthalten, aber in der Regel nicht zur öffentlichen Freigabe bestimmt sind. Daten mit mittlerer Auswirkung auf das Unternehmen (medium business impact, MBI) umfassen Informationen über das Unternehmen, die einzeln nicht zwingend vertraulich sein sind, aber durch Kombination oder Analyse wettbewerbsrelevante Erkenntnisse oder personenbezogene Informationen liefern, die zwar nicht von vertraulicher Natur sind, aber aus Datenschutzgründen nicht freigegeben werden dürfen. Daten mit großer Auswirkung auf das Unternehmen (high business impact, HBI) umfassen alles, was durch behördliche Vorschriften abgedeckt ist, die Reputation des Unternehmen oder von Einzelpersonen betrifft, zum Verschaffen von Wettbewerbsvorteilen genutzt werden könnte, von finanziellem Wert ist oder gegen Auflagen für vertrauliche Daten verstoßen könnte.

⁷ Azure Trust Center: <http://azure.microsoft.com/de-de/support/trust-center/>
Cloud Security Alliance: <https://cloudsecurityalliance.org>

Dann sollten Sie für jede Risikokategorie Richtlinienvorschriften festlegen. Beispielsweise ist für LBI möglicherweise keine Verschlüsselung vorgeschrieben. Bei MBI müssen Daten für die Übertragung verschlüsselt werden. Bei HBI müssen zusätzlich zur Verschlüsselung übertragener Daten auch ruhende Daten verschlüsselt werden. Möglicherweise müssen Sie zudem Überprüfungsanforderungen, Zugriffskontrolle und weitere Sicherheitsrichtlinien für diese Kategorien erstellen. Das Cloud-Strategieteam, das mit der IT-Sicherheitsgruppe zusammenarbeitet, könnte Anwendungen, die LBI-Daten verwalten, bei der Migration zur Cloud priorisieren, da sie das geringste Risiko darstellen. Für HBI-Daten wie personenbezogene Kundeninformationen (personally identifiable information, PII) kann eine Sicherheitsprüfung vor der Migration verlangt werden, was bei LBI-Anwendungen nicht unbedingt der Fall ist.

Unternehmensrisikomanagement

Wenn Sie ein Team für das Unternehmensrisikomanagement (enterprise risk management, ERM) beschäftigen, arbeiten Sie eng mit diesem zusammen, um die Auswirkung der Cloud auf die Risikomodelle zu bestimmen. Die meisten ERM-Teams verfügen über eine detaillierte, dokumentierte Liste der Unternehmensrisiken, deren Wahrscheinlichkeit und Auswirkungen. Als Reaktion auf diese Risiken werden die ERM-Teams Kontrollen einführen und Teams zusammenstellen, die das Risiko je nach Schweregrad beheben oder überwachen. Die Cloud wird wie jede andere bedeutende Neuerung das vorhandene Risikomodell verändern und neue Risiken bergen, die unbedingt untersucht und besprochen werden müssen. Im äußerst unwahrscheinlichen Fall eines Ausfalls des Cloud-Rechenzentrums sollten IT-Abteilungen die Georeplikation von Daten in Betracht ziehen, um das Risiko von Datenverlusten zu reduzieren.

Finanzmanagement

Ihr CFO und die Finanzabteilung Ihres Unternehmens müssen unbedingt in den Cloud-Migrationsplan eingebunden werden. Entwickeln Sie gemeinsam mit ihnen Kostenmodelle, die den lokalen IT-Betrieb (im Rechenzentrum) mit dem Cloud-Betrieb vergleichen. Zudem benötigen Sie Modelle, die zeigen, wie sich Kauf und Beschaffung neuer Hardware im Laufe der Zeit auswirken. Möglicherweise müssen Sie sogar Modelle entwickeln, die zeigen, wann und wie Rechenzentren geschlossen werden können.

Entwickeln Sie einige wichtige Maßnahmen, um die Einsparungen zu quantifizieren. Eine Maßnahme, die wir bei Microsoft einsetzen, wird als Kosten pro Betriebssysteminstanz (cost per operating system instance, Cost/OSI) bezeichnet. Wir beziehen dabei sowohl Anwendungen und Betriebssysteme auf Bare-Metal-Servern als auch solche ein, die als einzelne Metrik auf VMs ausgeführt werden. Cost/OSI umfasst Hardware, Lizenzen, Einrichtung, Netzwerk, Betriebsteam und – im Allgemeinen – alle Kosten für die Ausführung eines Betriebssystems und dessen Anwendungen in einem lokalen Rechenzentrum. Sie können Systeme bei Bedarf segmentieren: Wir setzten eine Metrik für kleine, mittelgroße, große und extragroße Bereitstellungen ein.

Mit dieser Metrik können Sie nun die Betriebskosten eines lokalen Systems mit denen eines Cloud-Systems vergleichen. Natürlich unterscheiden sich die Parameter für Cost/OSI in der Cloud und umfassen die Anwendung, die Anzahl der benötigten Kerne, den Speicherbedarf und den geschätzten Netzwerkdatenverkehr. Im Gegensatz zum lokalen Modell können Sie Server in der Cloud abschalten, wenn Sie sie nicht benötigen oder nutzen und somit Kosten verringern oder sogar komplett eliminieren.

Bestimmen Sie zunächst Ihre aktuellen Cost/OSI-Ausgaben als Basislinie. Dann können Sie Kosten für verschiedene Vorgänge in der Cloud prognostizieren. Die meisten Cloud-Dienstanbieter, darunter auch Azure, stellen Kalkulationstools zur Verfügung, die Sie beim Ermitteln Ihrer Cost/OSI unter verschiedenen Konfigurationen und Anforderungen unterstützen.

Erstellen Sie gemeinsam mit Ihrer Finanzabteilung mehrere Szenarien für Ihre Cloud-Migration, darunter auch aggressive, moderate und langsame Migrationspläne wie in Abbildung 5-4. Ein aggressiver Plan könnte z. B. vorsehen, im ersten Jahr 50 % Ihrer Workloads in die Cloud zu verschieben, ein moderater Plan könnte 30 % und ein langsamerer Plan nur 10 % vorsehen. Mit aggressiven Plänen können Sie größere Einsparungen erzielen, aber Sie müssen diese auch gegen größere Risiken und höhere Migrationskosten abwägen.

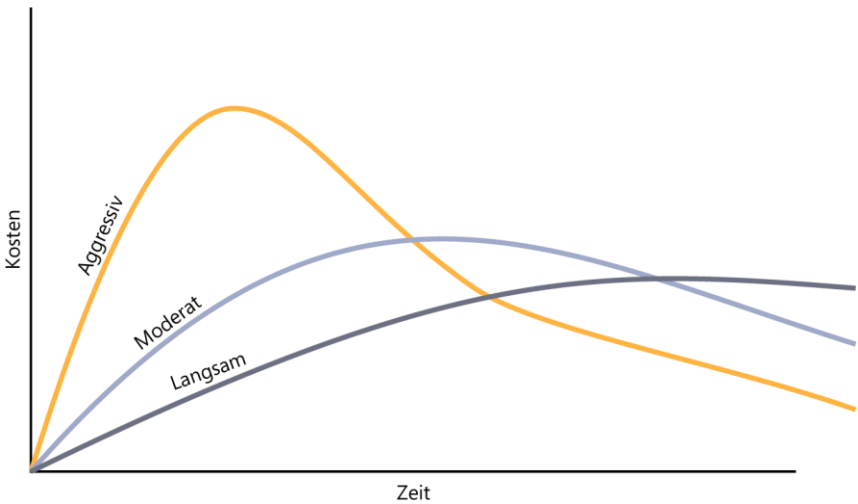


Abbildung 5-4: Nutzungsraten und Kosten

Natürlich muss die Finanzabteilung verstehen, dass der Wechsel in die Cloud mehr als nur Kosteneinsparungen bedeutet. Sie müssen die Daten des Unternehmens als wertvolle Ressource betrachten, deren Wert noch weiter gesteigert werden kann, wenn wir wissen, was wir damit tun können. Wenn Sie neue Datentypen verwenden, die Daten analysieren, um Erkenntnisse über Produkte, Kunden und Prozesse zu sammeln, häufig experimentieren, um zu ermitteln, wie wir maximalen Wert aus diesen Erkenntnissen ziehen können und diese Innovationen skalieren, können wir den Wert Ihrer Daten beträchtlich steigern. Diese Aktionen verbessern die Kontrolle und verringern die Risiken von Unternehmensprozessen – ein wichtiges Thema für alle CFOs. Je besser Sie den Mehrwert der Daten und Kosteneinsparungen durch den Umstieg auf die Cloud quantifizieren können, umso einfacher können Sie weitere wichtige Entscheidungsträger vom Umstieg überzeugen.

Operatives Geschäft

Die Cloud-Migration hat deutliche Auswirkungen auf den täglichen Betrieb in einer IT-Abteilung. Auch wenn die Anforderungen dieses Teams *funktionell* intakt bleiben, ändert sich die *Mechanik*, wie viele Funktionen ausgeführt werden, beträchtlich. Überlegen Sie, wie sich die folgenden Prozesse in einer cloudorientierten Welt verändern:

Prozess	Lokale Funktion	Cloud-Funktion
Systemüberwachung	Einsatz verschiedener Tools wie Microsoft System Center, um Anwendungen zu überwachen und bei Fehlern eine Root Cause Analysis (RCA) zu erstellen	Entwickler einbinden, um die Anwendungen in Echtzeit zu überwachen und die Auswirkungen von (z. B. täglichen oder sogar stündlichen) Updates (z. B. DevOps) schnell zu verstehen

Prozess	Lokale Funktion	Cloud-Funktion
Sicherheits-Operationen (SecOps)	Verwenden von Security Information und Event Management (SIEM)-Tools für die Analyse von Ereignissen und regelmäßige Prüfung von Ereignis Log-Dateien	Einsatz von Produkten wie Azure Security Center, um Bedrohungen zu verhindern, zu erkennen und abzuwehren
Datensicherung	Einsatz von lokalen Tools wie Microsoft System Center Data Protection Manager (DPM), um datenträger- oder bandbasierte Sicherungen zu erstellen	DPM für IaaS-VMs oder Azure Backup Services für PaaS zum Erstellen von Onlinesicherungen (optional mit Georeplikation) nutzen
Skalierbarkeit	Weitere Hardwareinstanzen (Server) im Rechenzentrum hinzufügen und bereitstellen, sicheren Betrieb und Netzwerkkonnektivität sicherstellen	Skalierungsoptionen <i>konfigurieren</i> , um durch Ermöglichen von Skalierung, Zuverlässigkeit und Resilienz automatisch auf Spitzen zu reagieren
Geschäftskontinuität/Testen der Notfallwiederherstellung	Benutzerdefinierte Skripts für Failover an alternative Rechenzentren nutzen	Tools wie Azure Site Recovery aktivieren, um ein skriptbasiertes, planmäßiges Failover auszuführen und Anwendungen sowie Speicher wiederherzustellen
Netzwerkconfiguration und -optimierung	Mit verschiedenen Tools die Netzwerkleistung analysieren und optimieren, Routerschleifen entdecken usw.	Ordnungsgemäße Abstimmung und Lastenausgleich von Hybrid-Netzverbindungen wie V-Nets und MPLS-Router („ExpressRoute“) sicherstellen
Identitätsbereitstellung und -entziehung	Benutzerverzeichnis (z. B. Active Directory) verwalten, ordnungsgemäßen Benutzerzugriff auf Ressourcen sicherstellen, Single Sign-On (SSO) aktivieren/erzwingen	Verzeichnis in die Cloud ausweiten und möglicherweise andere Authentifizierungsformen für bestimmte Anwendungen und Ressourcen nutzen

Diese Liste ist weder vollständig noch endgültig, sondern dient zur Veranschaulichung von verschiedenen Themen, denen sich das operative Team widmet.

Das operative Team wartet in der Regel eine zusätzliche Configuration Management Database (CMDB) für alle Hardwareressourcen. Die CMDB enthält viele relevante Inhalte für den Cloud-Migrationsprozess. Wie wir später sehen werden, enthält die CMDB Informationen wie die Größe der für eine bestimmte Anwendung erforderlichen Server, die typische Anzahl von VM-Instanzen, den verwendeten Speicher usw. Die Informationen in Kombination mit dem Portfoliomanagementsystem verschaffen Ihnen die Rohdaten zum Priorisieren der Anwendungsmigration.

Personal und die Entwicklung von Rollen

Die Migration zur Cloud zwingt die IT-Experten, ihre Rollen und Pflichten weiterzuentwickeln. Es wurde bereits viel darüber geschrieben, dass die Cloud IT-Arbeitsplätze gefährdet. Unserer Erfahrung nach ist das nicht der Fall. Stattdessen wandeln sich die IT-Rollen (siehe Abbildung 5-5) und verlagern sich von reinen IT-Funktionen hin zu wertvollen Beiträgen zum Unternehmen.

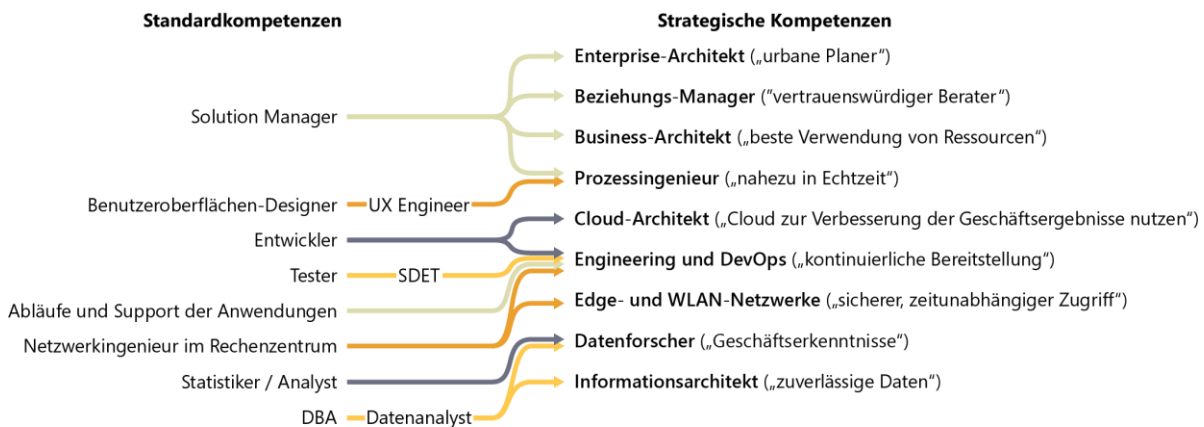


Abbildung 5-5: Die Entwicklung der IT-Rollen in Zeiten der Cloud

Vorhandene IT-Kompetenzen bleiben erhalten, aber sind von geringerer Bedeutung als die neueren, cloudorientierten Kompetenzen. Unternehmensarchitekturteams aus erfahrenen Technikern, Lösungsarchitekten und – in manchen Fällen – Kundenbetreuern verwalten das Portfolio ganzheitlich und wissen, wie der größtmögliche Geschäftswert aus großen Sammlungen von Anwendungen und Mitarbeitern gewonnen wird. Auf gewisse Weise sind sie die „urbanen Planer“ des Unternehmens. Unternehmensarchitekten, die quantitative Modelle verwenden und eng mit ihren Partnern in den jeweiligen Geschäftseinheiten zusammenarbeiten, untersuchen technische Ressourcen und Geschäftsprozesse in verschiedenen Unternehmensdomänen und planen ihre Entwicklung in der Zukunft. Prozessingenieure optimieren Unternehmensprozesse, die sie nach Möglichkeit in Echtzeit und ansonsten (gegebenenfalls) nahezu in Echtzeit ausführen. Erfahrungen mit Six Sigma sowie anderen Qualitätsmethoden sind hier von Vorteil.

Mit der Cloud kommt die größere Reichweite, und mit der größeren Reichweite die Anforderung, Anwendungen zu entwickeln, die produktiv und benutzerfreundlich zugleich sind. Designer von Benutzeroberflächen (UI) beschränken längst nicht mehr darauf, Menüs und Dialogfelder zu entwickeln. Sie müssen vielmehr sicherstellen, dass Onlinevorgänge effizient ausgeführt werden und, in Zeiten von Facebook, YouTube und Twitter, auch noch Spaß machen.

Cloud-Architekten konzentrieren sich darauf, eine oder mehrere Anwendungen zu planen und zu verbessern, die auf bestimmte Branchen wie das Finanzwesen ausgelegt sind, und arbeiten eng mit ihren Kollegen in den Bereichen Geschäftsarchitektur (Business Architecture, BA) und EA zusammen. Die Lösungsarchitekten sorgen für einen Überblick und eine Orientierung zur Entwicklung neuer Features und Funktionen in den Anwendungen. In der Regel handelt es sich um äußerst technikaffine Personen.

Zu den interessantesten – und am meisten diskutierten – Entwicklungen der Cloud-Migration zählt die Zusammenführung der zuvor separaten Bereiche Entwicklung und operatives Geschäft. Diese bezeichnet man als die *DevOps*-Bewegung. Durch das Verlagern von Anwendungen in die Cloud und die Möglichkeit, Anwendungen schnell und wiederholt bereitzustellen (teilweise werden neue Features täglich über agile Methoden hinzugefügt), beginnen die traditionellen Grenzen zwischen Entwicklern, Testern und operativem Team zu verblassen. Entwickler werden ihre Anwendungen in Staging-Umgebungen in der Cloud testen. Tester werden gezwungenermaßen versierter in Cloud-

Technologien werden als andere und häufig cloudbasierte Skripts oder Anwendungen in der Cloud schreiben – das macht sie ebenso zu Cloud-Entwicklern. Das operative Team wird immer weniger Hardwareressourcen wie Server und Netzwerke verwalten und zunehmend mit der Erstellung von automatisierten Konfigurationen, Bereitstellungsskripts, Insight portalen, Überwachungsskripts und Verwaltungsabläufen oder mit der Verwendung dieser Elemente beschäftigt sein, die von Cloud- oder Toolanbietern bereitgestellt werden. (DevOps werden in Kapitel 7 ausführlicher behandelt.)

Informationsarchitekten schließlich werden die Konsistenz der Datenmodelle im Unternehmen und deren Lebenszyklus sicherstellen. Eine Reihe gut gestalteter, dokumentierter und verwalteter Modelle – z. B. für „Kunden“- und „Produkt“-Datenentitäten – stellt unter anderem eine einfache Systemintegration und einheitliche Berichterstellung sicher.

Die Personalteam muss mit den relevanten Führungskräften zusammenarbeiten, um Vorbereitungs- und Schulungspläne für die betroffenen Personen zu erstellen. Fast alle Rollen in der IT werden sich weiterentwickeln. Für viele Rollen werden spezielle Schulungen erforderlich, beispielsweise zu neuen Tools oder Prozessen.

Entwicklung von Fähigkeiten

Stellen Sie sich über Entwicklung von Cloud-Umstellung in Phasen vor, mit jeweils zunehmenden Stufen an Ausbildung und Präzision. Ein für Sie nutzbares Framework umfasst drei Schulungsphasen (siehe Abbildung 5-6): Zunächst werden einzelne Personen geschult, dann werden Cloud-Teams aus geschulten Technikern zusammengestellt, die im letzten Schritt das gesamte Unternehmen weiterbilden.

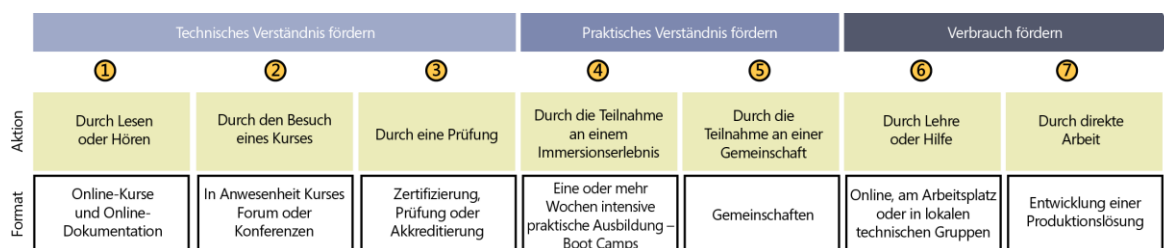


Abbildung 5-6: Kompetenzentwicklung

Fördern Sie in der ersten Phase (Abbildung 5-7) das technische Verständnis von Einzelpersonen, indem diese entweder online oder persönlich an Schulungen teilnehmen.

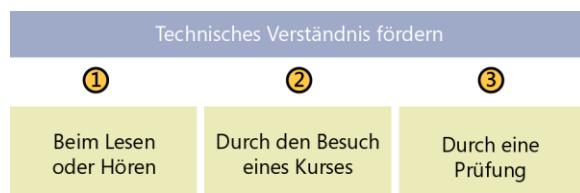


Abbildung 5-7: Technisches Verständnis fördern

Zahlreiche kostenlose oder günstige Onlinekurse für Azure existieren sowohl auf der Azure-Website (<https://azure.microsoft.com/en-us/community/training/>) als auch in der Microsoft Virtual Academy. Außerdem finden Sie ein umfassendes Set an Fortbildungsressourcen für Microsoft-Partner in der Azure-Fähigkeiten-Initiative (<https://blogs.partner.microsoft.com/mpn/new-cloud-trainings-for-next-generation-tech-professionals/>), und viele andere Organisationen bieten ähnliche Arten von Schulungen an.

In diesen Kursen erlernen Einzelpersonen grundlegende Fähigkeiten für die Cloud. Andere Schulungsformen (siehe Abbildung 5-8) helfen Ihren Teams dabei, gemeinsame Fähigkeiten zu entwickeln, um den Grundstein für Ihre Cloud-Praxis zu legen.



Abbildung 5-8: Entwicklung Ihrer Cloud-Praxis

Mit immersiven Erfahrungen wie Boot-Camps können Ihre Teams für einen ganzen Tag in die Cloud eintauchen, deren Konsequenzen für Ihr Unternehmen kennenlernen und an einer Vielzahl von Communities teilnehmen, um ihre Fähigkeiten zu erweitern.

Natürlich geht nichts darüber, selbst Hand anzulegen, entweder durch die Leitung oder Unterstützung eines Teams bei der Entwicklung und Bereitstellung von Cloud-Anwendungen (Abbildung 5-9) oder einfach durch die Übernahme einer Cloud-orientierten Position.

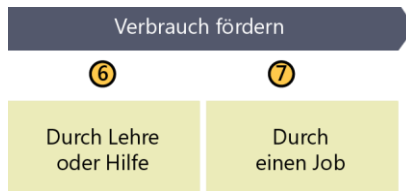


Abbildung 5-9 Ausbau der Fähigkeiten Ihres Teams

Welche Schulungsarten sind relevant für Ihre Teams? Hier sehen Sie einen Beispielkatalog mit Microsoft-Kursen. Anhand dieser Liste können Sie die in Abbildung 5-10 genannten Cloud-Rollen entwickeln.

Cloud-Verwaltung	Daten & Analytik*	Cloud-Entwicklung*	DevOps
<ul style="list-style-type: none"> • Microsoft Azure Grundlagen • Microsoft Azure für AWS Experten • Microsoft Azure Virtuelle Maschinen • Microsoft Azure Virtuelle Netzwerke • Microsoft Azure Identität • Microsoft Azure Speicher • Microsoft Azure Sicherheit und Compliance • Managing Azure Workloads • Microsoft Azure App Dienstleistungen • Datenbanken in Azure • Migration von Workloads in Azure • Anwendungsbereitstellung und Management 	<ul style="list-style-type: none"> • Verarbeitung von Big Data mit Hadoop in Azure HDInsight • Implementierung der Echtzeitanalyse mit Hadoop in Azure HDInsight • Implementierung prädiktiven Lösungen mit Spark in Azure HDInsight • Verarbeitung von Big Data mit Azure Data Lake Analytik • Verarbeitung von Echtzeit-Datenströmen in Azure • Orchestriert Big Data mit Azure Data Factory • Liefern eines Data Warehouse in der Cloud • Entwicklung von NoSQL-Lösungen in Azure • Die Entwicklung Big Data-Lösungen mit Azure Maschinelles Lernen • Provisioning-Datenbanken in Azure und SQL Server • Daten wiederherstellen in Azure und SQL Server • Daten sichern in Azure und SQL Server • Verwalten von Organisationsdatenquellen mit Azure Daten Katalog 	<ul style="list-style-type: none"> • IoT Lösungen entwickeln mit Azure IoT Hub • Azure App Konfiguration • Erstellen einer Angular Web App auf Azure • Entwickeln von Azure App Servicekomponenten 	<ul style="list-style-type: none"> • DevOps auf Azure Paas • Kontinuierliche Integration und Bereitstellung • DevOps Testing • Infrastruktur als Code* • Konfiguration* • Mobile DevOps* • Anwendungsüberwachung und Rückmeldeschleifen*

*Kurs(e) kommt bald

Abbildung 5-10 Verfügbare Schulungen für Azure

Mit einem durchdachten Ansatz für die Entwicklung von Fähigkeiten können Sie nicht nur Einzelpersonen in Ihrem Unternehmen fachgerecht schulen, sondern auch die Effektivität ganzer Teams verbessern.

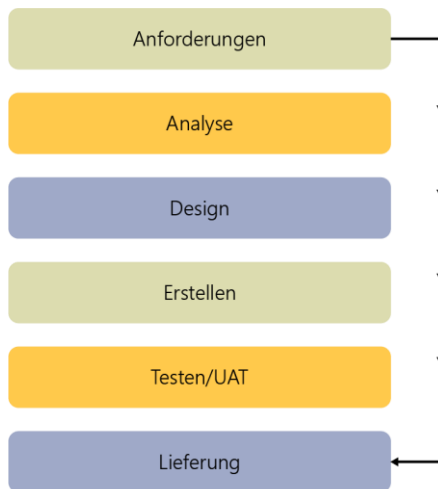
Anwendungsteams

Anwendungsteams werden zu den unterschiedlichsten Themen konsultiert. In der Regel stellen diese Teams die erforderlichen Informationen für den Anwendungskatalog oder das Portfolioverwaltungssystem bereit (wird später besprochen), mit denen Prioritäten bei der Anwendungsmigration gesetzt werden.

Des weiteren besprechen Sie mit ihnen, welche technischen Auswirkungen das Ausführen ihrer Anwendungen in der Cloud hat. Wenn eine Anwendung im Rechenzentrum „mitteilungsfreudig“ ist (also bei Erledigung einer Aufgabe viele Meldungen sendet und empfängt), kann die Latenz beim Verschieben in ein externes Cloud-Rechenzentrum zu Verzögerungen führen. Um dieses Problem zu beheben, werden Anwendungsteams versuchen, die Anwendung zu aktualisieren oder zu einer Highspeed-Leitung mit zusätzlicher Bandbreite raten. Wenn Sie eine Cloud-Datenbank nutzen, unterliegt diese möglicherweise bestimmten Größeneinschränkungen, die jedoch mit bestimmten Ansätzen wie Datenbank-*Sharding* behoben werden können (ein Datenbankshard ist eine Datenpartition in einer Datenbank, jeder Shard wird auf einer separaten Datenbankserverinstanz gehostet).

Anwendungsteams sollten die langfristigen Möglichkeiten einer cloudorientierten Anwendung kennen. Beispielsweise sind zur Neugestaltung einer Anwendung in PaaS oder einer Sammlung sogenannter *Microservices* (in Kapitel 11 genauer beschrieben) Aufmerksamkeit und Fachkenntnisse gefragt.

Was die Methodik angeht, sollten sich Anwendungsteams überlegen, ob ein traditioneller *Wasserfall*-Ansatz (siehe Abbildung 5-11) oder eine *agile* Methodik mit vielen kurzen Entwicklungssprints mit Feedback und potenziellen Kurskorrekturen besser geeignet ist. Bei bestimmten Anwendungstypen wie der Finanzbuchhaltung, bei der möglicherweise strenge Vorschriften über die funktionellen Möglichkeiten bestimmen, kann ein Wasserfallansatz sinnvoll sein. Projekte nach dem Wasserfallansatz enthalten in der Regel eine detaillierte, umfassende Spezifikation, die von Projektmanagern überprüft werden kann.



* Linearer Ansatz

Abbildung 5-11: Traditioneller Wasserfallansatz für die Softwareentwicklung

Heutzutage erfordern jedoch immer weniger Anwendungen einen solchen Grad an Präzision, und die meisten Anwendungen profitieren von kurzen Entwicklungsphasen gefolgt von Usability-Tests und Feedback, einem Markenzeichen der agilen Entwicklung (siehe Abbildung 5-12). Auf diese Weise bekommen die Benutzer ein Gefühl für die Anwendung und können neue Funktionen anfordern, die Entfernung anderer Funktionen vorschlagen usw. In vielen Fällen ergibt die agile Methodik eine Lösung, die die Bedürfnisse der Nutzer weit besser erfüllt als der lineare Wasserfallansatz.

Diese Diskussion ist wichtig, da die Cloud viel schnellere Entwicklungs- und Bereitstellungszyklen ermöglicht und sich daher hervorragend für die agile Entwicklung eignet.

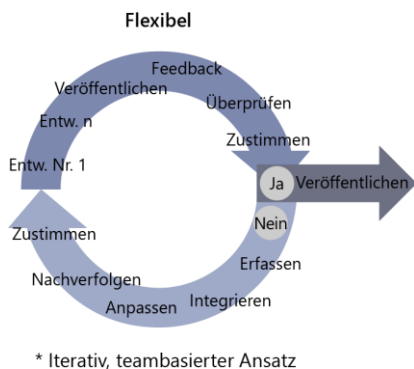


Abbildung 5-12: Cloud-Softwareentwicklung

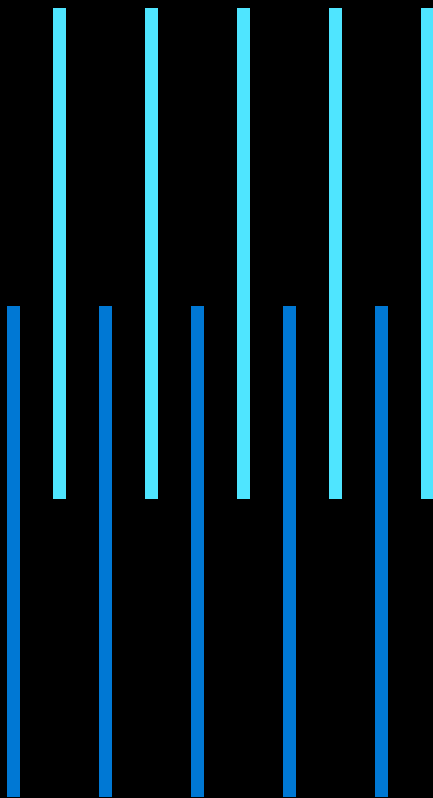
Geschäftseinheiten

Ihre Geschäftseinheiten sollten ebenfalls befragt werden. Einige werden die Veränderung begrüßen, andere lehnen sie möglicherweise ab, da eine solche Veränderung wie bereits besprochen auch Risiken birgt. Wenn Sie Ihnen auf verständliche Weise erklären, wie Sie diese Risiken meistern werden, können Sie ihnen viele ihrer Ängste nehmen. Natürlich werden die erwarteten Vorteile wie Kosteneinsparungen, größere Reichweite und schnellere Bereitstellung ihren Appetit anregen. Durch eine frühe Einbeziehung Ihrer Fürsprecher und Entwicklung echter Anwendungen, die die Vorteile veranschaulichen, können Sie auch die anderen überzeugen.

Beachten Sie deren Terminkalender. Für Führungskräfte gibt es einige wichtige Termine, an denen ihre Systeme verfügbar sein müssen, z. B. die Finanzberichtsperiode oder im E-Commerce der Zeitraum um Feiertage wie den Black Friday in den USA. Anschließend können Sie um diese Termine herum planen.

Kapitel 6

Portfolioanalyse



Wie genau setzen wir Prioritäten für die Migration von Anwendungen in die Cloud? Um herauszufinden, welche Anwendungen wann und wie verschoben werden sollten, muss ein umfassender, von der IT verwalteter Anwendungskatalog erstellt werden. Anschließend kann die relative Bedeutung der einzelnen Attribute (Geschäftskritikalität oder Umfang der Systemintegration) abgewogen und die Prioritätenliste entwickelt werden.

Entwicklung des Katalogs

Möglicherweise müssen viele Attribute von Dokumentklassifizierungstypen über Serveranzahlen bis hin zu Protokollen beachtet werden. Häufig ist es sinnvoll, diese wie in Abbildung 6-1 gezeigt in Verwaltungssets allgemeiner Attribute einzuteilen. Wie Sie in der Abbildung sehen, sind die wichtigsten Kriterien in diesem Fall Leistung, Architektur, finanzielle Betrachtungen, Risiko, Prozesse, Sicherheit und Compliance.

Viele Unternehmen verwenden bereits ein Portfolioverwaltungssystem, in dem eine solche Liste gepflegt wird. Diese Systeme können in der Regel für Cloud-Zwecke eingesetzt oder erweitert werden. Andere Unternehmen verwenden möglicherweise ein Ad-hoc-Tool wie eine Tabellenkalkulation. Beide Methoden können effektiv sein.

Anwendungseigenschaften oder Attribute sollten aus geschäftlicher („top-down“, von oben nach unten) und technischer („bottom-up“, von unten nach oben) Perspektive betrachtet werden. Dies ist wichtig, da die Daten aus unterschiedlichen Nutzergruppen stammen. Beim Top-down-Ansatz fragen Sie sich, wohin die Anwendungen oder Workloads verschoben werden sollten, und der Bottom-up-Ansatz beschreibt, wohin diese Elemente verschoben werden können. In den folgenden Abschnitten werden die einzelnen Elemente zusammen mit den relevanten Attributen beschrieben.

Leistung	Architektur	Finanzen	Risiko	Abläufe	Sicherheit und Compliance
Flexibilität	Benutzer- oberfläche	Betriebskosten	Unternehmens- bezogen	Business Continuity	Gerichtsstand
Skalierbarkeit	Zugangs- punkte (Mobil oder offline)	Geschäftswert	Unternehmens- kritisch	Tools/ Integration	Richtlinien
Ressourcen- intensität	Anwendung		Technisch	Bereitstellung	Datenschutz
Latenz	Komplexität		Ressource		Verschlüsselung
Durchsatz	Größe		Vertraglich		
	Anwendungs- lebensdauer		Überwachung		
	Daten				
	Größe (strukturiert)				
	Anforderungen (unstrukturiert)				
	Komplexität				
	Infrastruktur				
	Hardware- lebensdauer				

Abbildung 6-1: Bewertungskriterien

Top-down-Portfolioanalyse

Bisher haben wir den Migrationsprozess als systematischen Ansatz besprochen und dabei objektive und subjektive Metadaten geprüft, um zu bestimmen, wohin Anwendungen oder Workloads verschoben werden sollten. Diese Top-down-Bewertungsmethode ist ein strategischer Ansatz, der von der Planung und von Ihren detaillierten Analyse- und Modernisierungsanforderungen beeinflusst wird.

In Abbildung 6-2 sehen Sie, dass bei der Top-down-Bewertung zunächst die bereits erwähnten Sicherheitsaspekte wie die Kategorisierung von Daten (hohe, mittlere oder geringe Auswirkung) sowie Compliance, Datenhoheit und Sicherheitsrisiken geprüft werden. Anschließend werden die aktuelle Komplexität, Authentifizierung, Datenstruktur, Latenzanforderungen sowie Kopplung und Anwendungslebensdauer der Architektur geprüft. Danach prüft die Top-down-Bewertung die operativen Anforderungen der Anwendung, z. B. Servicelevel, Integration, Wartungsworkflows, Überwachung und Erkenntnisse. Nachdem all diese Aspekte analysiert und in Betracht gezogen wurden, erhalten Sie ein Ergebnis, das den relativen Aufwand für die Migration dieser Anwendung in jede dieser Cloud-Plattformen (IaaS, PaaS und SaaS) abbildet.

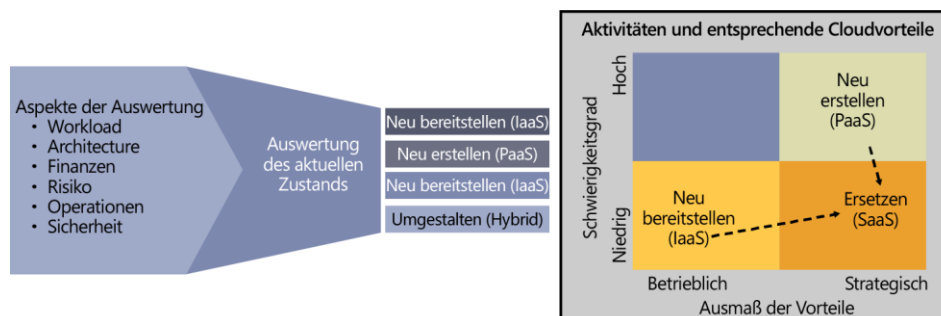


Abbildung 6-2: Top-down-Bewertung der aktuellen Anwendung

Zudem lernen Sie bei der Top-down-Bewertung die finanziellen Vorteile der Anwendung wie betriebliche Effizienz, Gesamtbetriebskosten, Rendite oder andere Finanzmetriken besser kennen. Die Bewertung prüft auch die Saisonabhängigkeit der Anwendung (zu manchen Jahreszeiten steigt der Bedarf stark) und allgemeine Computerlast. Außerdem prüft diese Methodik die Support-Benutzertypen (Anfänger/Experte, immer angemeldet/gelegentlich angemeldet usw.) sowie die dafür benötigte Skalierbarkeit und Elastizität. Zum Abschluss des Tests werden die möglichen Business-Continuity - und Resilienzanforderungen der Anwendung sowie deren Abhängigkeiten im Fall einer Dienstunterbrechung geprüft.

Die beiden Teile des Prozesses ergeben eine Anwendungsbewertung, die die Balance zwischen dem Migrationsaufwand für die einzelnen Plattformen und den potenziell daraus zu gewinnenden Vorteilen abbildet. Abbildung 6-3 zeigt den gesamten Prozess.

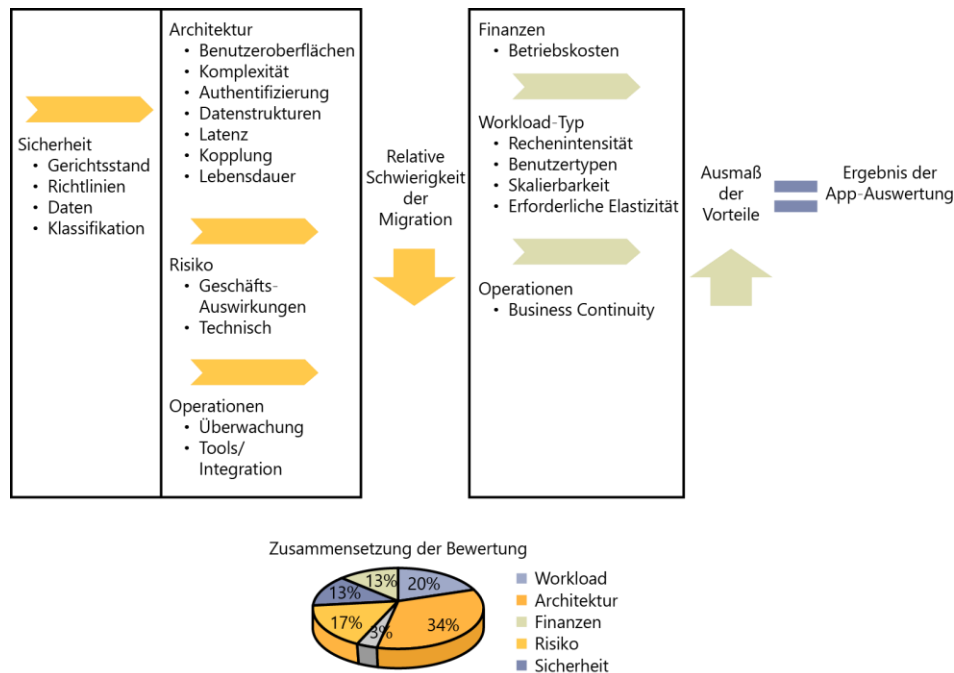


Abbildung 6-3: Top-down-Bewertungsprozess

Mit den Ergebnissen aus der Top-Down-Methode können Sie herausfinden, welche Anwendungen den größten potenziellen Wert haben und sich am besten für die Migration eignen, und mit diesen Anwendungen beginnen. Sie können diese Liste auch mit den schnellen Gewinnen kombinieren, die auf Anwendungen von geringerem potenziellem Wert basieren und auch besser für die Migration geeignet sind. Nachdem Ihre Organisation die entsprechenden Erfahrungen gesammelt hat, die richtigen Tools und Prozesse gewählt hat und Vertrauen in ihre Methoden gewonnen hat, ist es an der Zeit, sich den schwieriger zu migrierenden Anwendungen mit höherem potenziellem Wert zu widmen. Übrig bleiben die schwieriger zu migrierenden Anwendungen mit geringem potenziellem Wert. Abbildung 6-4 bildet diesen Prozess ab.

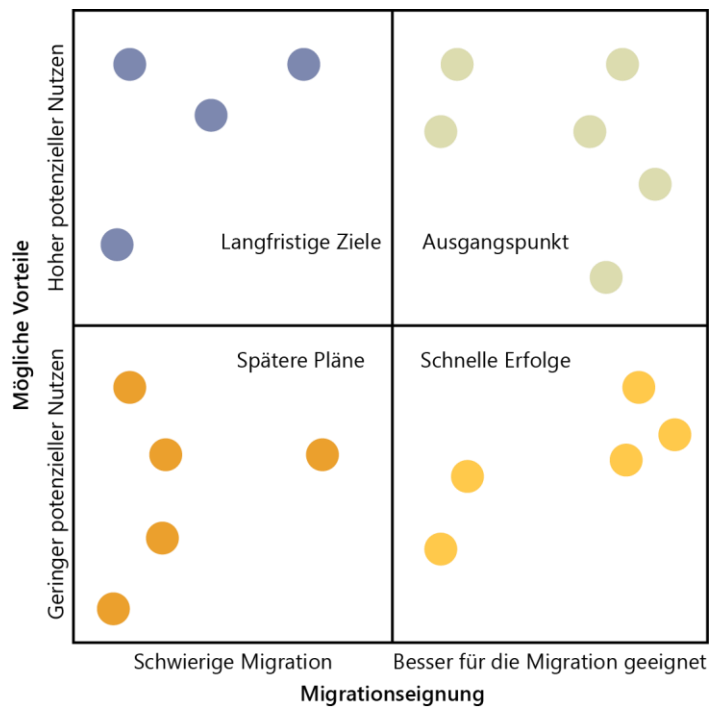


Abbildung 6-4: Migrationseignung von Anwendungen versus möglicher Vorteil

Bottom-up-Portfolioanalyse

Es gibt einen weiteren Ansatz, der taktischer und technischer ist und sich stärker auf die Anforderungen konzentriert. Wie bereits erwähnt, analysiert der Top-down-Ansatz, wohin eine Anwendung verschoben werden *sollte*. Beim nächsten Ansatz fragen wir uns, wohin eine bestimmte Workload verschoben werden *kann* (basierend auf den technischen Anforderungen).

Der Bottom-down-Ansatz (Abbildung 6-5) erfolgt zeitgleich mit Ihrer Top-down-Planung und eröffnet Einblicke in die technische Eignung einer Anwendung für die Migration. Viele dieser Informationen können in der Regel aus einer Configuration Management Database (CMDB) gewonnen werden. Unternehmen verwenden diese Methode, um weitere Insight in den Top-down-Ansatz zu gewinnen.

Die Art von Anforderungen, die bei der Bottom-up-Bewertung geprüft werden, decken auch die Anwendung oder den Dienst ab: maximaler Speicher, maximale Anzahl von Prozessoren (CPU-Kerne), maximaler Speicherbedarf des Betriebssystems, maximale Datenlaufwerke, Netzwerkschnittstellenkarten (NICs), IPv6, Netzwerklastenausgleich, Clustering, Betriebssystemversion, Datenbankversion (falls erforderlich), unterstützte Domänen, externe Komponenten, Softwarepakete usw.

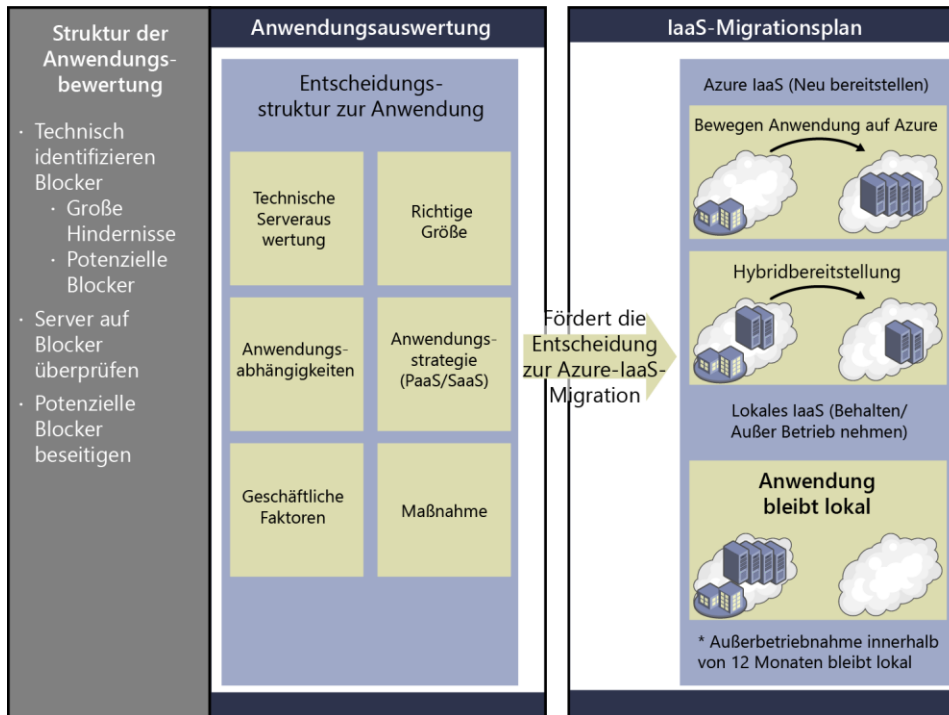


Abbildung 6-5: Beispiel einer Bottom-up-Bewertung für IaaS

Mit jedem Tag scheinen Cloud-Plattformen unterschiedliche Anwendungsportfolios immer besser bewältigen zu können. Server mit 16 oder 32 CPU-Kernen sind allgegenwärtig, und riesige Mengen an Arbeits- und persistentem Speicher stehen zur Verfügung. Jedoch können Sie auch weiterhin auf Anwendungen stoßen, die Sie aus technischen Gründen gerade nicht verschieben können⁸, oder bei denen Sie warten sollten, bis weitere Cloud-Funktionen verfügbar sind.

Bei der Bottom-up-Planung katalogisieren Sie die technischen Aspekte Ihrer Anwendungen wie Betriebssystemtyp, Version, Anzahl der erforderlichen Prozessoren, Bedarf an Arbeits- und persistentem Speicher, Anzahl der Laufwerke usw. Wenn Sie die Größe einer Anwendungsdatenbank und ihre Datentypen kennen, können Sie fundierte Entscheidungen treffen, ob Sie z. B. eine cloudorientierte relationale Datenbank wie Microsoft Azure SQL-Datenbank, Microsoft SQL Server oder Oracle in einer virtuellen Maschine (VM) oder sogar eine NoSQL-Datenbank einsetzen sollten.

Ihre vorhandenen Integrationssysteme werden – zumindest vorübergehend – von Cloud-Migrationen beeinflusst. Dokumentieren daher Sie die potenzielle Auswirkung auf diese Systeme. Sie müssen wissen, welche Anwendungen miteinander vernetzt werden, ob bei Integrationsprozessen eine bestimmte Reihenfolge beachtet werden muss, wie viele Daten wie häufig verschoben werden und welche Architektur Ihre ETL-Tools (Extrahieren, Transformieren und Laden) verwenden. Die Komplexität Ihrer Anwendungsprozesse sollte einen wichtigen Faktor beim Priorisieren von Cloud-Migrationszielen darstellen.

Zudem implementieren Cloud-Anbieter heutzutage Optionen für Business-Continuity und Notfallwiederherstellung, darunter Failover zu verschiedenen Rechenzentren, redundanten Datenspeicher und Onlinesicherungen. Lernen Sie die Angebote und ihre Funktionen kennen und machen Sie sich bewusst, wie diese sich auf Ihre Anwendungsanforderungen auswirken.

⁸ Beispiel: Anwendungen, die von veralteten Features in Betriebssystemen abhängig sind, auf Betriebssystemen ausgeführt werden, die in der Cloud nicht unterstützt werden, oder die auf schlechter Programmierung basieren, wie etwa hartcodierte IP-Adressen.

Eine Vielzahl an Tools, die Ihnen helfen kann, den aktuellen Status Ihrer Anwendungen zu bewerten. Wie bereits erwähnt, wird ein Portfoliomanagementsystem von großer Hilfe beim Auflisten und Zuordnen Ihrer Anwendungen sein. Die Microsoft System Center Suite umfasst eine CMDB sowie Überwachungs- und Statusmanagement-Funktionen, die Sie bei der Bestimmung des Systemstatus unterstützen.⁹ Das Microsoft Assessment and Planning Toolkit ist ein Starterpaket mit mehreren nützlichen Funktionen zur Bewertung vorhandener IT-Umgebungen. Das MAP erleichtert die automatische Inventur und Bewertung von Anwendungen, um die grundlegende Eignung und VM-Größenanforderungen zu ermitteln.¹⁰ Außerdem stehen verschiedene externe Anwendungen und Programme für ähnliche Funktionen zur Verfügung.

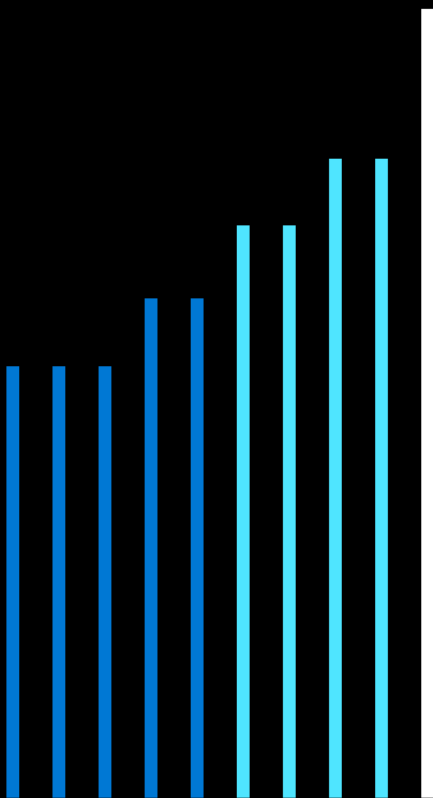
Die Art der Informationen, die Sie mit diesen Hilfsmitteln erfassen, dient objektiven Faktoren wie Eignung von Hardware/VM sowie Anwendung/Workload für die Cloud-Migration. Diese Tools sind eine sehr hilfreich bei der automatisierten Erfassung von Metadaten zu Ihren Anwendungen und Betriebssysteminstanzen.

⁹ <http://www.microsoft.com/de-de/server-cloud/products/system-center-2012-r2/>

¹⁰ <http://technet.microsoft.com/de-de/solutionaccelerators/gg581074>

Kapitel 7

Entwicklung und
Ausführen des Plans



Jedes große Unterfangen beginnt mit einem Plan. Mit einem wohlverstandenen und nach Kriterien priorisierten Portfolio ist es an der Zeit, die eigentliche Migration von Anwendungen in die Cloud zu beginnen. In diesem Kapitel betrachten wir die Entwicklung des tatsächlichen Plans und setzen ihn anschließend um.

Beginnen Sie zunächst mit Entwicklungs- und Testbereichen

Bevor Sie sich der Migration von Produktionsanwendungen widmen, macht es Sinn, zunächst Ihre Entwicklungs-/Testumgebungen zu verschieben. Dafür gibt es eine Reihe guter Gründe:

- **Entwicklungs/Testumgebungen sind teuer.** Mit dem Umzug dieser Umgebungen können Sie teils beträchtliche Kosteneinsparungen erzielen. Oft gibt es drei separate Umgebungen pro Anwendung, völlig losgelöst von der Produktionsumgebung: eine Entwicklungsumgebung, eine Testumgebung, die von der QA für Komponenten- und automatisierte Tests verwendet wird, und eine Umgebung für Benutzerakzeptanztests (User Acceptance Testing, UAT). Diese Umgebungen umfassen zahlreiche Server und virtuelle Maschinen (VMs), die im Rechenzentrum nicht mehr benötigt werden.
- **Ihre Teams erhalten können sich mit den Migrations-Tools vertraut machen.** Ihre Teams lernen die Migrations-Tools kennen, ohne die Produktionsumgebung zu gefährden. Wenn Sie anschließend die Produktionsumgebung migrieren, profitieren Sie von den zuvor gewonnenen Erfahrungen.
- **Entwickler sind in der Regel toleranter gegenüber Problemen als Benutzer.** Mit anderen Worten, wenn etwas schief geht, sind die Produktionsbenutzer nicht betroffen, und Entwickler und IT-Mitarbeiter können aus den Fehlern lernen.

- **Die Reihenfolge ist weniger wichtig.** Wie Sie sehen werden, sollten beim Umzug von Produktionsanwendungen die in Kapitel 6 erstellten Priorisierungsrichtlinien beachtet werden. Dies ist bei Dev- und Testanwendungen weniger wichtig, obwohl Compliance-Bestimmungen für geschützte Daten wie personenbezogene Informationen für Entwicklungs- und Testumgebungen ebenso gelten wie in Produktionsumgebungen (daher werden bei der Entwicklung oft anonymisierte Daten verwendet).

Der Cloud-Migrationsplan

Kehren wir nun zu Ihren Produktionsanwendungen zurück. Ihre Kartierung vom aktuellen Status zum gewünschten Status bildet die Grundlage für Ihren Cloudmigrationsplan. Der Migrationsplan ergänzt diese Kartierung um Prioritäten und Sequenzen.

Definieren Sie Prioritäten in Ihrem Plan auf der Basis von Unternehmens-, Hardware-, Software- und anderen technischen Faktoren. Ihr Team für Geschäftsbeziehungen sollte mit dem Betriebsteam und den beteiligten Unternehmenseinheiten eine gemeinsam vereinbarte Prioritätenliste erstellen. Abbildung 7-1 zeigt die Prinzipien, die Sie beim Erstellen von Priorisierungsrichtlinien verwenden können.

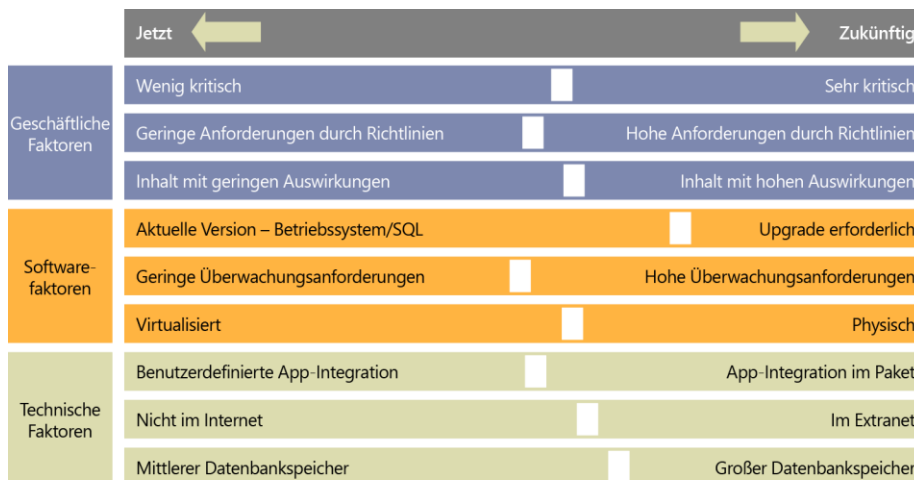


Abbildung 7-1: Strategie zum Setzen von Migrationsprioritäten

Bei der Migrationsreihenfolge für Ihre Workloads sollten Sie mit weniger komplexen Projekten beginnen und die Komplexität nach dem Umzug weniger komplexer Projekte schrittweise steigern. Wie auch bei der Durchführung eines Pilotprojekts gewinnen Sie beim Umzug von weniger komplexen Anwendungen mit geringeren Geschäftsrisiken wertvolle Erkenntnisse, die Sie auf komplexere, unternehmenskritischere Migrationen vorbereiten.

Ihr Cloud-Migrationsplan ist mehr ein Prozess als ein statisches Plandokument. Grundsätzlich ist Ihr Plan eine Kompilierung mehrerer kleiner Pläne zur Migration jeder Abteilungsworkload, die auf der erstellten Sequenz basieren. Die Migrationen folgen in der Regel diesem Muster:

1. **Analyse** Mit diesem Prozess identifizieren Sie die Lücken zwischen dem Ist-Zustand und dem Zustand, der für den Umzug der Workload in die Cloud erforderlich ist. Diese Lücken können von Änderungen an der Architektur der Workload bis zur vollständigen Neuentwicklung des Programms reichen. (Informationen dazu finden Sie im Abschnitt „Die fünf Pfeiler der Modernisierung“ in Kapitel 3.) Zudem ist bei vielen älteren Programmen ein beträchtlicher Aufwand erforderlich, um ihre Leistung und Skalierbarkeit zu verbessern. Identifizieren Sie diesen Aufwand bei Ihrer Analyse der Workload.

Bei der Analyse sollten Sie sich umfassend mit den Sicherheits- und Compliance-Auswirkungen der jeweiligen Anwendung vertraut machen und sicherstellen, dass alle personenbezogenen und sonstigen Informationen identifiziert werden. Arbeiten Sie bei Bedarf mit Ihren Teams für

Informationssicherheit und Risikomanagement zusammen, um entsprechende Kontrollmechanismen zu schaffen (dieses Thema wird in Kapitel 9 ausführlich behandelt).

2. **Anwendungsmigration** Wenn Sie entscheiden, dass eine bestimmte Workload in die Cloud verschoben werden soll, *entwickeln Sie idealerweise eine Version der Workload mit einer minimalen Menge an Daten, damit die Anwendung in der Cloud funktioniert, oder erstellen Sie eine neue Version der Anwendung in der Cloud.* Wenn die Anwendung bereits auf einer VM ausgeführt wird, kann die VM möglicherweise ohne weitere Änderungen einfach in die Cloud verschoben werden. Im Allgemeinen können viele lokale Anwendungen mit wenigen oder gar keinen Änderungen in Microsoft Azure ausgeführt werden. Dies bedeutet jedoch nicht unbedingt, dass die Anwendung für Leistung, Skalierbarkeit und Sicherheit optimiert ist. Daher müssen Sie die Anwendung unter Umständen in einem gewissen Umfang unter Anwendung moderner serviceorientierter Prinzipien umgestalten und neu erstellen.
3. **Netzwerk** Wie in Kapitel 10 ausführlich besprochen, können lokale Anwendungen auf viele verschiedene Arten sicher mit der Cloud verbunden werden. Diese Möglichkeiten reichen von einem einfachen virtuellen privaten Netzwerk (Virtual Private Network, VPN) bis hin zu einer dedizierten Leitung (z. B. Azure ExpressRoute) mit jeweils unterschiedlichen Leistungs- und Preischarakteristiken.
4. **Datenmigration** Dieser Vorgang ähnelt der Anwendungsmigration darin, dass die Datenstruktur ohne weitere Änderungen entweder in einen relationalen (Azure SQL Database, SQL Server in Azure VM) oder einen nicht relationalen (Blob, Tabelle, Warteschlange, Azure CosmosDB usw.) Speicherort in der Cloud verschoben werden kann. Manche Varianten dieser Migration sind sehr einfach und können mithilfe eines Assistenten wie etwa dem SQL Server Azure-Migrations-Assistenten ausgeführt werden.

Unter Umständen müssen Sie jedoch das Datenmodell als neue Azure SQL-Datenbank neu erstellen, damit Sie von den Verbesserungen der Leistung, Skalierbarkeit, Resilienz und Sicherheit profitieren können. Wenn Sie Daten zwischen lokalen Datenbanken und einer SQL-Datenbank oder zwischen verschiedenen SQL-Datenbankservern synchronisieren möchten, richten Sie den SQL-Datensynchronisierungsdienst ein, und konfigurieren Sie ihn. Zusätzlich *empfiehlt sich die Einrichtung und Konfiguration eines Plans für die Wiederherstellung der Daten im Falle von Benutzerfehlern oder Naturkatastrophen.*

5. **Optimierungen und Tests** Führen Sie nach dem Umzug Ihrer Anwendungen und Daten nach Azure unbedingt Funktions- und Leistungstests durch. Testen Sie Ihre Anwendung in dieser Phase in der Cloud, und stellen Sie sicher, dass sie korrekt funktioniert. Vergleichen Sie daraufhin die Leistungsergebnisse, die Sie lokal und in Azure erzielt haben. Beheben Sie daraufhin eventuell aufgetretene Fehler in Bezug auf Features, Funktionen, Leistung oder Skalierbarkeit in Ihrer Cloud-Anwendung.
6. **Ausführung und Verwaltung** Nach der Test- und Optimierungsphase folgt die Einrichtung und Implementierung der Anwendungsüberwachung und -nachverfolgung mit Azure Application Insights, mit denen Sie Telemetriedaten für Ihre Anwendung sammeln und analysieren können. Diese Daten können Sie zum Debuggen, Beheben von Problemen, Messen der Leistung, Kontrollieren der Ressourcennutzung sowie zur Datenverkehrsanalyse, Kapazitätsplanung und Überwachung verwenden.

Verwenden Sie die Microsoft Operations Management Suite zum Verwalten von Anwendungen, die sowohl lokal als auch in der Cloud ausgeführt werden. Die Operations Management Suite bietet eine einzige Übersicht über alle Ihre Anwendungen, unabhängig davon, wo diese gehostet werden.

Diese sechs Migrationsphasen werden für jede Workload ausgeführt, die verschoben werden soll. Daneben gibt es auch einen iterativen Prozess, der umfassender ist als jede Migration, und mit dem

Sie Anwendungen verschieben können, die Ihre anfänglichen Mindeststandards auf Grundlage von Priorität und Reihenfolge erfüllen. Nachdem die anfängliche Gruppe verschoben wurde, können Sie damit beginnen, die Eignung weiterer Anwendungen und Hardware zu verbessern, indem Sie Upgrades für die Betriebssystem- und SQL-Versionen durchführen, alle Sicherheitspatches auf den neuesten Stand bringen, Anwendungen oder physische Computer in VMs verschieben, Probleme aufgrund von mehreren IP-Adressen beheben usw.

Tools

Für den Umzug von VMs nach IaaS können Sie eine Reihe von leicht verfügbaren Tools von verschiedenen Anbietern verwenden. Der integrierte Business Continuity und Disaster Recovery (BC/DR)-Dienst von Azure, Azure Site Recovery, umfasst eine Suite von Tools zum Verschieben von VMs (einschließlich VMware VMs) von einem lokalen Rechenzentrum in die Cloud und zwischen verschiedenen Cloud-Regionen. Für Websites können Sie den Azure Websites-Migrationsassistenten verwenden, um einen Internet Information Server (IIS) mühelos in die Cloud zu verschieben. Der Data Migration Assistant (Abbildung 7-2) unterstützt Sie bei der Planung der Migration einer lokalen SQL Server-Datenbank in eine Azure SQL Database.

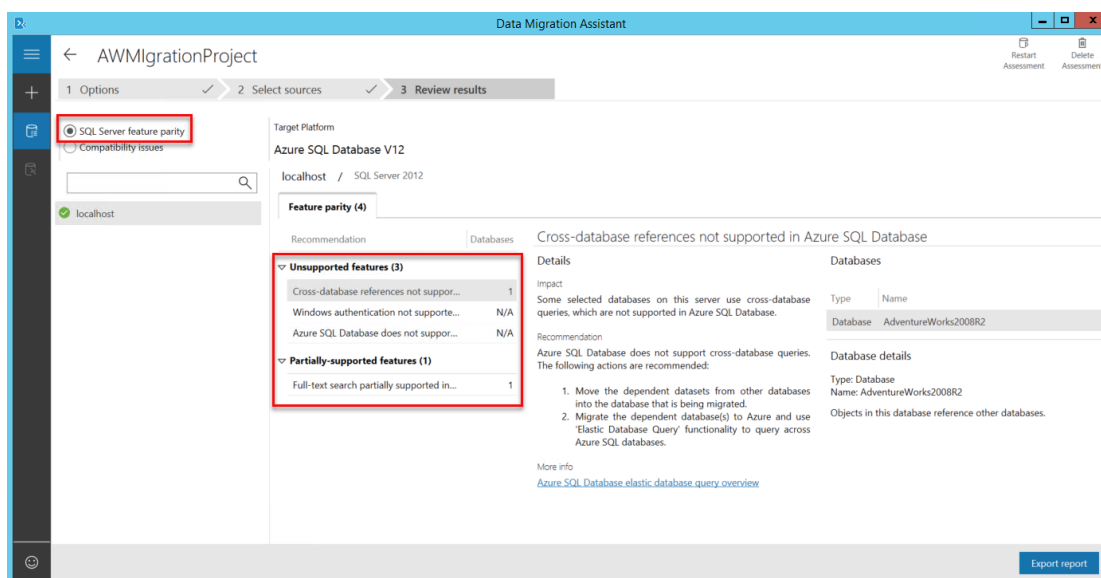


Abbildung 7-2: Azure Data Migration Assistant: Screenshot

Abonnementverwaltung

Wenn Sie damit beginnen, Live-Anwendungen in der Cloud einzusetzen, sollen Sie sich mit der Abonnementverwaltung vertraut machen. Obwohl es verlockend ist, das gesamte Unternehmen in einem Cloud-Abonnement zusammenzufassen, bedeutet dieses Modell beträchtliche Effizienzeinbußen: Mit einem einzigen Abonnement ist es schwierig, Abrechnungen nach Anwendungen und/oder Kostenstellen bzw. Abteilungen zu erstellen. Außerdem ist die Verwaltung einer großen Anzahl von Anwendungen – Test-, Produktionsumgebungen usw. – aufwändig, und es kann passieren, dass der Administrator für ein einzelnes Abonnement von den neuen Anfragen für VMs und andere Ressourcen überlastet wird.

Es ist in der Regel effektiver, Abonnements für einzelne Kostenstellen oder sogar Anwendungen oder Anwendungsgruppen (z. B. Vertriebsanwendungen) zuzuweisen. Auf diese Weise erhalten Sie einen besseren Einblick in die Kosten einzelner Funktionen, und CIOs können Kostenziele zu den einzelnen Gruppen zuweisen, die separat verwaltet werden können.

Für große Unternehmen sollten Sie nach Möglichkeit eine Cloud-Governance-Hierarchie (siehe Abbildung 7-3) einrichten, um Transparenz und Zuständigkeiten zu verbessern.

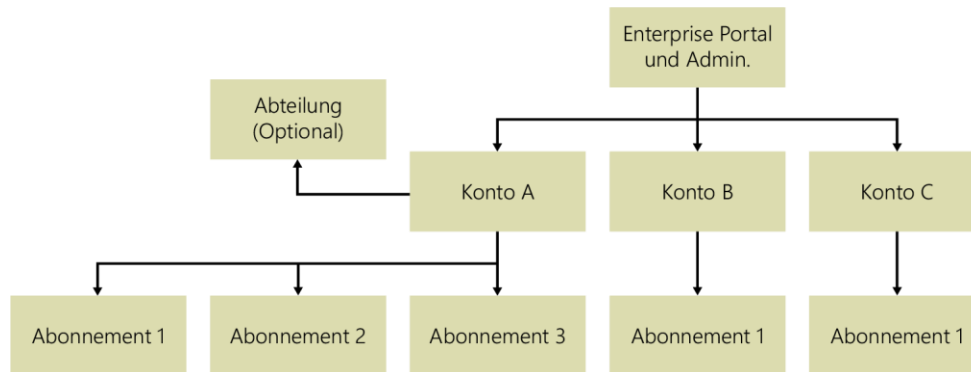


Abbildung 7-3: Governance-Hierarchie für die Abonnementverwaltung

Dieses Modell verwendet ein einziges unternehmensweites Portal, in dem alle Kosten im gesamten Unternehmen sichtbar sind. Konten auf Abteilungsebene können ein oder mehrere Abonnements enthalten, beispielsweise für Kostenstelle oder für einzelne Lösungsbereiche.

Microsoft Power BI bietet Ihnen eine komfortable Möglichkeit zur Darstellung Ihrer Abonnements und deren Nutzung (siehe Abbildung 7-4).

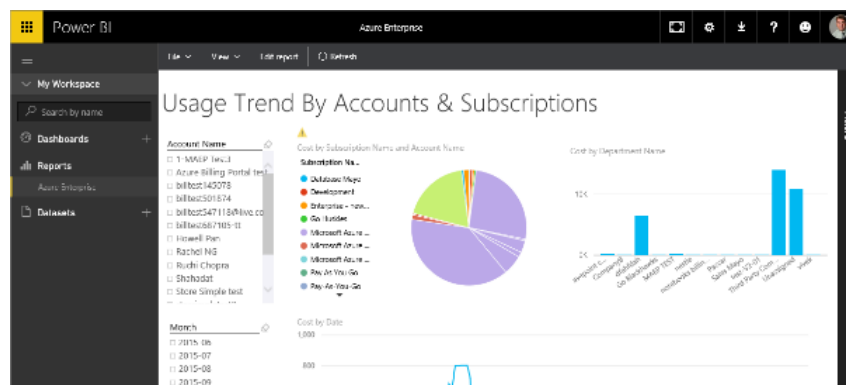


Abbildung 7-4: Azure-Nutzung und Kostenberichte in Power BI

Die Erfahrung von Microsoft IT

Als Microsoft IT im Jahr 2009 mit der Cloud-Migration begann, war der Ablauf ähnlich. Zunächst wurden die Instanzen des Betriebssystems und die Anwendungs-Workloads katalogisiert. Diese Auswertung umfasste sowohl quantitative Daten, die größtenteils von Tools abgerufen wurden, als auch qualitative Daten, die teilweise von Tools abgerufen wurden und zudem auch sowohl vom Betriebsteam als auch vom Team für Geschäftsbeziehungen analysiert werden mussten. Die letztere Metadatenkategorie umfasste Beziehungen, Abhängigkeiten und Integrationspunkte.

Anschließend hat Microsoft IT die geeigneten Betriebssysteminstanzen und die geeigneten Workloads/Anwendungen mit der jeweils höchsten Priorität identifiziert. Diese ersten Migrationskandidaten wurden anschließend reduziert, indem geschäftskritische Systeme entfernt wurden, deren Migration später durchgeführt werden sollte, wenn mehr Erfahrung gesammelt wurde. Anschließend wurden diese ersten Kandidaten priorisiert, und es wurde eine Reihenfolge erstellt, in der weniger komplexe Anwendungen bevorzugt wurden. Anwendungen, die auf aktualisierten VMs ausgeführt wurden, hatten eine höhere Priorität als Anwendungen, die auf physischen Computern oder älteren VMs ausgeführt wurden. Einige Anwendungen wurden aus verschiedenen Gründen als nicht geeignet identifiziert (die meisten dieser Beschränkungen gehören 2017 der Vergangenheit an) und in ein optimiertes lokales Rechenzentrum verschoben.

Nach Abschluss der ersten Migrationen hat Microsoft IT sich darauf konzentriert, die Eignung weniger gut geeigneter Betriebssysteminstanzen und Workloads zu verbessern. So wurden Betriebssysteminstanzen mit älteren Betriebssystemen oder Datenbankversionen aktualisiert, weitere auf physischen Computern befindliche Anwendungen wurden zu virtuellen Computern verschoben, und mehr geschäftskritische Anwendungen wurden als geeignet eingestuft. Anwendungen und Workloads, bei denen eine umfassende Überholung erforderlich war, wurden als Dienste in Azure erneut erstellt.

Der Ablauf ist dabei der folgende (siehe auch Abbildung 7–5):

1. Identifizieren geeigneter Hardware (Betriebssysteminstanzen) nach Azure Server-, Speicher- und RAM-Beschränkungen
2. Identifizieren Sie geeignete Anwendungen, entfernen Sie Anwendungen mit sensiblen Daten fürs Erste, setzen Sie kritische und komplexe Anwendungen für später an, und planen Sie die passende Kapazität, um mehr Anwendungen einzubeziehen.
3. Erweitern der geeigneten Hardware sowie der Anwendungen durch Folgendes:
 - Virtualisierung weiterer Server
 - Expansion in weitere Regionen
 - Einbeziehen von nach außen gerichteten Apps

Einbeziehen von Anwendungen mit sensiblen Daten („High Business Impact“ oder HBI, siehe Abbildung)

- Aktualisierungen (Betriebssystem, SQL)
- Erhöhen der Beschränkungen für Azure-VMs

4. Entwicklung neuer Anwendungen als Dienste für SaaS IT.

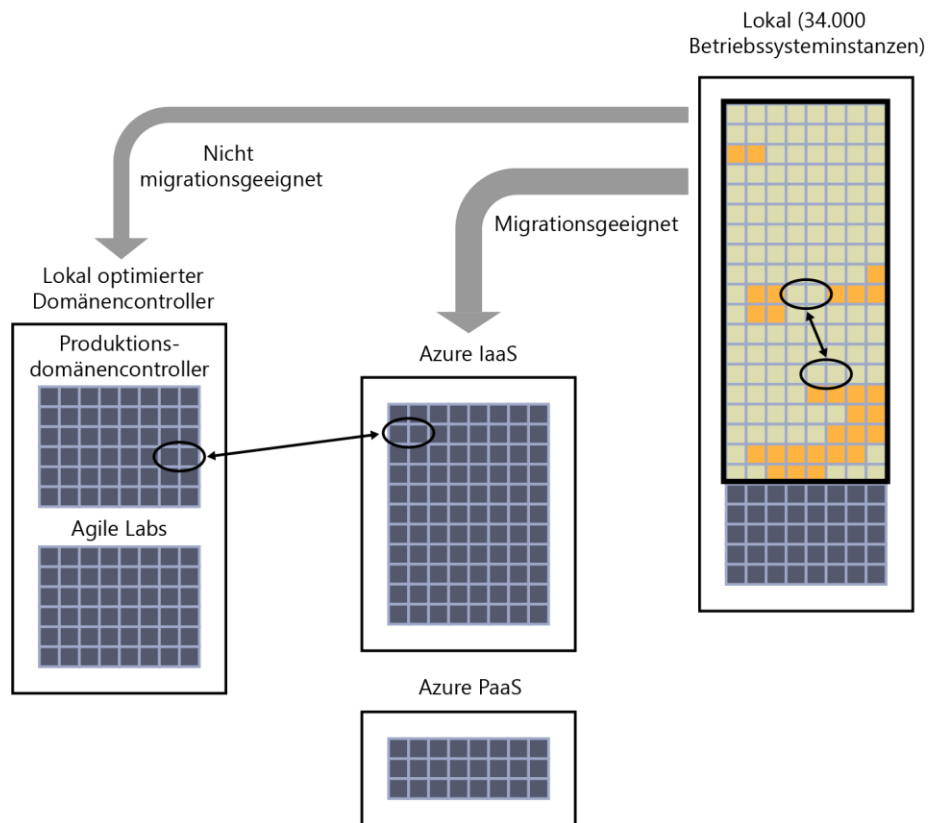
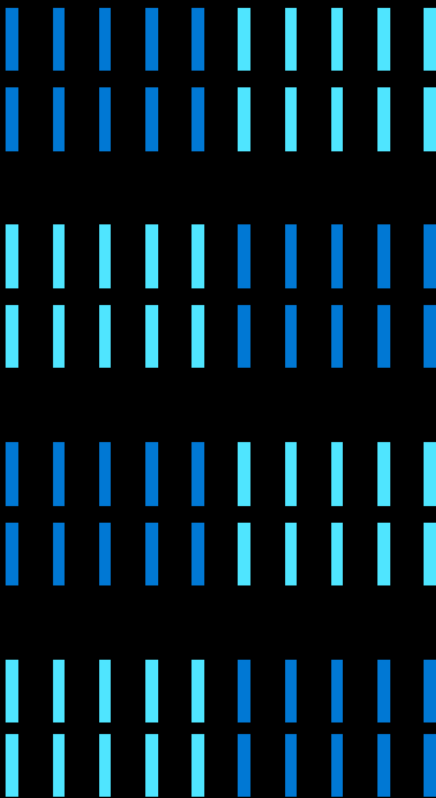


Abbildung 7-5: Implementieren des Plans

Kapitel 8

DevOps macht Teams produktiver



Die Entwicklung, Konfiguration, Bereitstellung, Verwaltung und Aktualisierung von Anwendungen in der Cloud eröffnet viele neue Möglichkeiten, um die Produktivität von Teams zu verbessern und Kosten zu senken. Die bislang getrennten Teams von IT-Software-Entwicklern und operativen Mitarbeitern kommen zusammen, um den Umzug von Anwendungen in die Cloud nahtlos, schnell und effizient zu gestalten. In diesem Kapitel betrachten wir, wie DevOps-Teams Cloud-Ressourcen für Entwicklung und Test bereitstellen und anschließend, wenn die Ressourcen nicht mehr benötigt werden, freigeben können. Wir sprechen auch darüber, wie DevOps Infrastruktur als Code behandeln, um Bereitstellungen und Updates schnell und sicher abzuwickeln.

Nutzung der Cloud für Entwicklung und Tests

Es ist noch nicht besonders lange her, dass Tests eines der größten Hindernisse für die IT-Produktivität waren. Vor der Live-Schaltung mussten Anwendungen getestet werden, zunächst von den Entwicklern und Testern unter stark kontrollierten Umständen, und anschließend „live“ mit echten Benutzern im Rahmen der Benutzerakzeptanztests. Die Compliance-Prüfung fand normalerweise etwa zur gleichen Zeit statt.

Dieses Entwicklung- und Testmodell brachte zahlreiche Probleme mit sich. In der Produktion traten häufig Fehler auf, die in den Entwicklungs- und Testphasen nicht bemerkt wurden. Warum? Häufig lag dies daran, dass sich die Konfiguration der Produktionsumgebung auf irgendeine Weise von den Entwicklungs-/Testumgebungen unterschied. Möglicherweise war die Hardware anders konfiguriert. Vielleicht unterschieden sich die „echten“ Daten qualitativ von den Testdaten. Vielleicht war die Belastung unerwartet hoch. In all diesen Fällen unterscheidet sich die Entwicklungs-/Testumgebung auf irgendeine Weise vom tatsächlichen Anwendungsfall, was im Nachhinein offensichtliche Probleme verursacht hat.

Wenn die gesamte Entwicklung lokal geschieht, ist es manchmal sehr schwierig, eine Umgebung zu erstellen, die die Produktionsbedingungen abbildet. Die Beschaffung ausreichender Hardware konnte beispielsweise enorme Kosten verursachen. Die Simulation der Benutzerlast kann zu ungenauen Ergebnissen führen, wenn sich Hardwareumgebungen und Softwarekonfigurationen voneinander unterscheiden, usw.

Die Nutzung der Cloud für Entwicklungs-/Testumgebungen bietet zahlreiche Möglichkeiten. Ein zentraler Aspekt von Cloud Computing ist die Möglichkeit, Kapazitäten bereitzustellen, zu nutzen und anschließend freizugeben, wenn sie nicht mehr benötigt werden. Dieses Modell eignet sich hervorragend für Entwicklung und Tests.

Mit Microsoft Azure DevTest Labs (Abbildung 8-1) können Sie Entwicklung und Tests in der Cloud mit einem kontrollierten Self-Service-Modell durchführen. Mit Dev/Test Labs können Sie Server für die Entwicklung zuweisen. Sie können einen separaten Satz von Servern mit einer kontrollierten Konfiguration zu einer bestimmten Tageszeit (z. B. nachts) hochfahren, um Tests durchzuführen, und diese Server nach Abschluss der Tests oder zu einer bestimmten Uhrzeit wieder freigeben. Wie auch in einem lokalen Lab können Sie mithilfe von Richtlinien festlegen, welche Art von Testcomputern verwendet wird, wie viele Computer pro Benutzer zugewiesen werden dürfen, und wann das Projekt für das jeweilige Lab endet (Ablaufdatum).

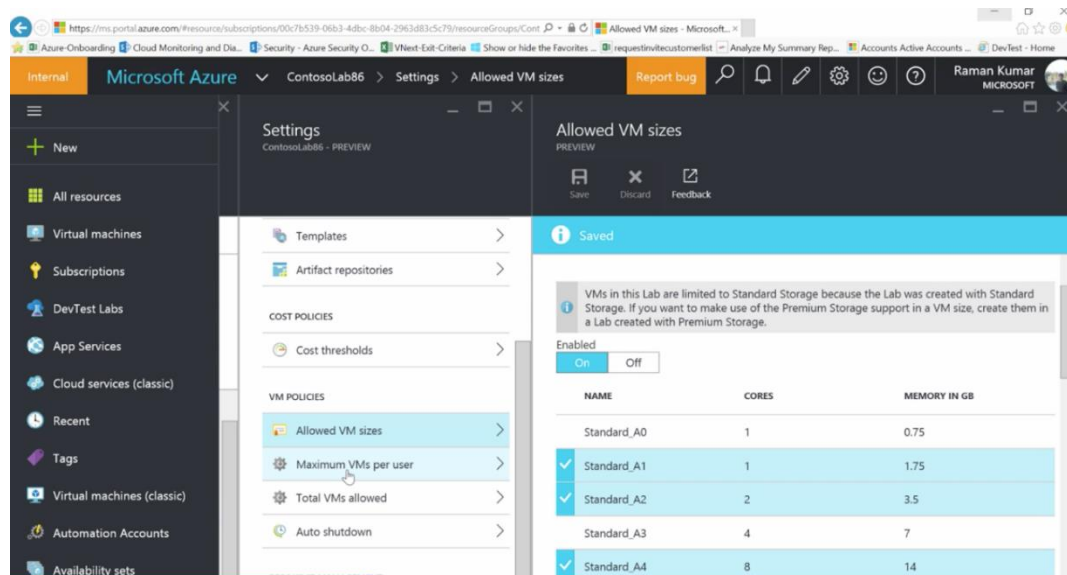


Abbildung 8-1: Festlegen zulässiger VM-Größen für Dev/Test Labs

Um sicherzustellen, dass jedes Mal die korrekte Umgebung getestet wird, können Sie virtuelle Maschine Abbilder mit der benötigten Software vorab erstellen, um häufige Fehler zu reduzieren oder zu eliminieren, die durch unterschiedliche Umgebungen oder Konfigurationen entstehen. Außerdem können Sie gängige Tools wie Telerik Fiddler (Tool für die Analyse des Netzwerkdatenverkehrs), PowerShell-Skripts, Protokollfunktionen oder andere Tools in die Testumgebung integrieren. Diese Tools sind sehr hilfreich für die Diagnose von aufgetretenen Problemen. Zuletzt können Sie die Konfiguration der Umgebung jederzeit ändern, um unterschiedliche Konfigurationen schnell und einfach zu testen.

Die DevOps-Revolution

Seit Jahrzehnten standen Kostenkontrolle und Risikomanagement für die Unternehmens-IT im Mittelpunkt. Sämtliche Hardware- und Softwarekomponenten wurden sorgfältig abgerechnet, und größere Käufe waren nur nach zahlreichen Prüfungsschritten durch verschiedene Gruppen im gesamten Unternehmen möglich, um sicherzustellen, dass das Geld sinnvoll ausgegeben wurde.

Der Entwicklungsprozess war ebenso starr. „Account Manager“ haben gemeinsam mit ihren Geschäftspartnern Anforderungsdokumente erstellt. Eine funktionale Spezifikation wurde geschrieben und dem Entwicklungsteam vorgelegt, das daraufhin ein Design oder eine technische Spezifikation erstellt hat. Wenn die Dokumentation nach mehreren Prüfungen abgezeichnet wurde, begann die Entwicklung. Zu verschiedenen Meilensteinen wurde der Code an das Testteam übergeben, das anschließend Funktionstests durchgeführt und Fehlerberichte erstellt hat. Schließlich wurde der Code an die Benutzerakzeptanztests übergeben, und erst nach Abschluss dieser Phase wurde die Software in die Produktion überführt.

Dieser „Wasserfallansatz“ für die Softwareentwicklung ist zwar leicht verständlich und in einer Projektmanagementanwendung leicht nachzuverfolgen, steckt jedoch voller Probleme und Effizienzhemmnisse. Die Entwicklung und Bereitstellung neuer Versionen dauerte oft Monate oder Jahre. Die Bereitstellung von Anwendungen schlug fehl, weil die Testumgebungen nicht einheitlich konfiguriert waren, oder weil die Menge und Art des Datenverkehrs im Produktionsbetrieb nicht den Erwartungen entsprach. Aufgrund der großen Anzahl der beteiligten Gruppen – Entwicklung, Test, Operations – hat die Behebung kritischer Probleme inakzeptabel lange gedauert. Viele IT-Abteilungen mussten sich die Kritik anhören, sie sehen „zu teuer und zu langsam“.

Mit zunehmender Verbreitung von internetorientierten Computing-Methoden wurde das kosten- und risikenorientierte Modell durch den Fokus auf *Geschwindigkeit* abgelöst, d. h. einer Nachfrage nach (sehr viel) häufigeren neuen Versionen. E-Commerce-Webseiten bieten beispielsweise ständig neue Produkte und neue Kaufanreize an, und müssen daher sehr häufig aktualisiert werden, möglicherweise sogar Hunderte von Male *pro Tag*.

Eine Lösung wurde gesucht und gefunden.

Kontinuierliche Integration und Bereitstellung

In Anlehnung an Lean Manufacturing-Methoden begannen zahlreiche Akteure, agilere Entwicklungsstrategien auszuprobieren, um die lästigen Dokumentationsphasen zu überspringen und stattdessen kurze Coding-„Sprints“ zu verwenden, in denen ein Teil der Funktionen implementiert, mit tatsächlichen Benutzern getestet und das Feedback in den nächsten Sprint integriert wurde. Anstatt die Softwareentwicklung als eine Abfolge von Phasen zu betrachten, verwendeten diese Pioniere eine fortlaufende, sich wiederholende Pipeline aus Entwicklung, Test und Bereitstellung.

Automatisierte Tests haben viele der bisherigen manuellen Funktionstests abgelöst (der entsprechende Jobtitel lautet nicht mehr *Tester*, sondern *Softwareentwickler für Tests* [Software Development Engineer in Test, SDET]). Beim Einchecken von neuem Code wird eine Reihe automatisierter Tests ausgelöst, um sicherzustellen, dass keine neuen Probleme entstanden sind. Andernfalls wird der Entwickler benachrichtigt und der Checkin abgelehnt. Dieser Prozess wird auch als *kontinuierliche Integration* (Continuous Integration, CI) bezeichnet.

Außerdem zeigte sich schnell, dass die Skripts und Konfigurationen zur Kontrolle der Bereitstellung *selbst aus Code bestehen* und mit Versionskontrollmechanismen, Fehlerüberwachung usw. als solcher behandelt werden können. Den Unternehmen dämmerte der inzwischen berühmte Spruch, „Infrastruktur als Code“ zu behandeln. In Azure wird die Infrastruktur beispielsweise vom Azure Resource Manager in JavaScript Object Notation (JSON) beschrieben. Der folgende Codeausschnitt dient zur Benennung einer Linux-VM in ARM:

```
{
  "type": "Microsoft.Compute/virtualMachines",
  "name": "demoLinuxVM",
  ...
}
```

Dieser radikale Umbruch fand auf kultureller wie auch auf technologischer Ebene statt und ist heute als DevOps bekannt, da er die bislang separaten Rollen von Entwicklung, Test und Operations vermischt. Beim Einchecken von neuem Code werden automatisierte Tests durchgeführt, und nach Bestehen der Tests wird der Code automatisch in der Produktionsumgebung bereitgestellt. Dies wird als auch als kontinuierliche Bereitstellung (Continuous Deployment, CD) bezeichnet. Mit dieser Vorgehensweise können manche Anwendungen bis zu 200 Mal pro Tag bereitgestellt werden.

Überwachung und Instrumentierung

Mit DevOps können Entwickler auch die Instrumentierung in den Code integrieren, um jederzeit Telemetriedaten zu erhalten und die Anwendungsintegrität überwachen zu können. Azure Application Insights umfasst nicht nur APIs, sondern auch ein Dashboard, in dem Sie Telemetriedaten inklusive Warnungen überwachen können. Diese Daten können anschließend an ein Repository wie Hadoop oder dessen von Azure verwaltete Dienstversion HDInsight (siehe Kapitel 12) weitergeleitet werden, um Nutzungsmuster und andere Trends zu analysieren. In Abbildung 8-2 sehen Sie eine Application Insights-Analyse der durchschnittlichen Verweilzeit von Benutzern auf einer Website.

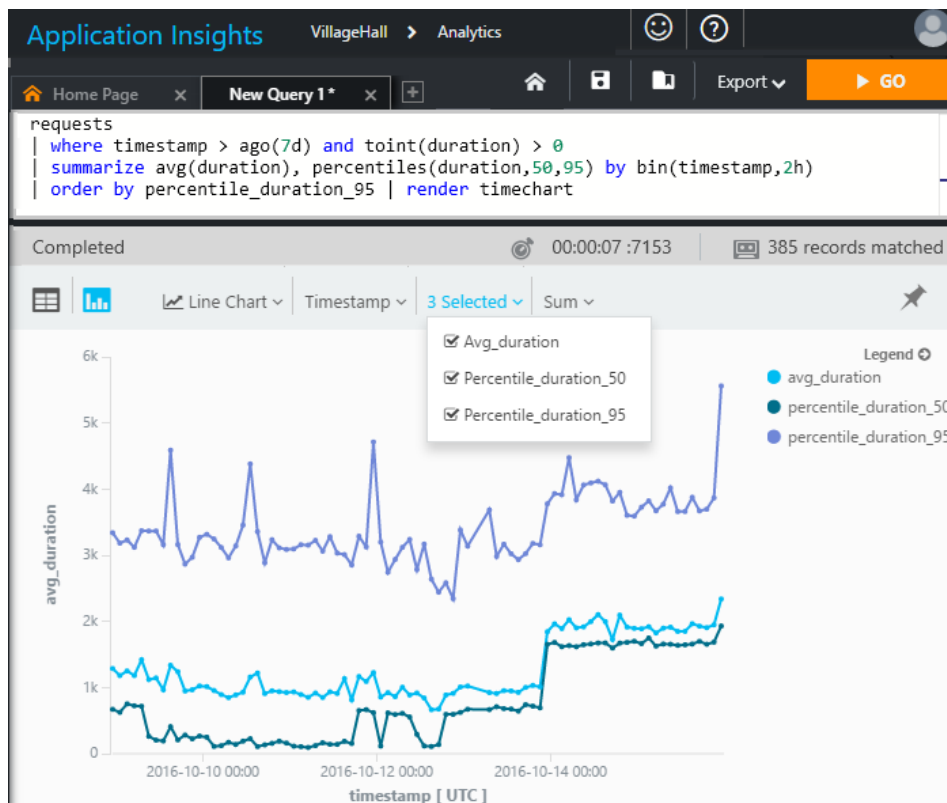


Abbildung 8-2: Durchschnittliche Verweilzeit von Benutzern in Application Insights

Hier sehen Sie den neuen Entwicklungszyklus: Programmierung, Benutzertests, automatisierte Tests, automatische Bereitstellung gefolgt von Laufzeit-Feedback aus der Telemetrie und bei Bedarf Feinabstimmung der Bereitstellungsparameter.

Wie wäre es mit einer einheitlichen Ansicht sämtlicher relevanter Metriken für Ihre Anwendung? Der neu angekündigte Azure Monitor (siehe Abbildung 8-3) vereint Aktivitäts Log-Dateien (zur Nachverfolgung aller auf Azure-Ressourcen ausgeführten Operationen), Metriken und Diagnose Log-Dateien und enthält Tools, mit denen Sie Regeln für Warnungen konfigurieren können.



Abbildung 8-3: Azure Monitor

Dazu können Sie die Azure Log Analytics nutzen, die Daten aus vielen verschiedenen Überwachungsquellen sammelt und aggregiert, allerdings mit einer Verzögerung von 10 bis 15 Minuten. Die Log Analytics ist ein Teil der Operations Management Suite und bietet eine ganzheitliche IT-Management-Lösung für Azure sowie für lokale und externe cloudbasierte Infrastrukturen. Sie erhalten umfangreichere Tools zur Analyse von Daten aus mehr Quellen, können komplexe Abfragen für alle Log-Dateien ausführen und proaktive Warnungen für festgelegte Bedingungen erhalten. Sie können sogar benutzerdefinierte Daten im zentralen Repository erfassen, um diese Daten anschließend abzufragen und darzustellen.

Optimieren Sie Ihre Infrastruktur mit DevOps

Der Umzug Ihrer Anwendungen in die Cloud kann auch zu unerwarteten Resultaten führen: Möglicherweise stellen Sie fest, dass Sie in der Cloud *mehr ausgeben* als für Ihre lokale Lösung.

Wie kann das passieren? Immerhin befasst sich ein Großteil dieses Buchs damit, wie Ihr Unternehmen mit der Cloud Zeit und Geld sparen kann!

Diese unerwünschte Situation tritt häufig auf, wenn die Konfiguration von Anwendungen nach dem ursprünglichen Umzug in die Cloud mehr oder weniger exakt beibehalten wird. Ein Beispiel: Wenn Ihre Anwendung in Ihrem lokalen Rechenzentrum auf acht Servern läuft, dann werden beim ursprünglichen Umzug höchstwahrscheinlich acht Infrastructure as a Service (IaaS)-Server bereitgestellt.

Allerdings lief Ihre Anwendung ursprünglich nur auf acht Servern, um die Last zu Spitzenzeiten verarbeiten zu können: ein Großteil der Prozessoren wird nur zu einem Bruchteil ausgelastet.

In diesem Fall zeigen sich die Stärken von Cloud und DevOps. Durch die fortlaufende Überwachung mit Tools wie dem bereits erwähnten Application Insights können Sie Tag für Tag (oder bei Bedarf auch Minute für Minute) herausfinden, was in Ihren Anwendungen vor sich geht.

Häufig stellen Sie dabei fest, dass ein beträchtlicher Anteil Ihrer Server nur zu einem Bruchteil ausgelastet ist und Sie wichtige Einsparungen vornehmen können.

Wenn Sie beispielsweise feststellen, dass Ihre acht Server mit jeweils sechs Prozent CPU-Auslastung laufen, können Sie diese Last auf zwei Server konsolidieren und den Rest an den Pool zurückgeben. In diesem Fall werden Ihnen nur zwei Instanzen in Rechnung gestellt. Wenn Sie diesen Ansatz auf Ihr gesamtes Anwendungsportfolio in der Cloud anwenden, können Sie beträchtliche Einsparungen erzielen.

Im Beispiel in Abbildung 8-4 wird eine bestimmte IaaS-Anwendung in Microsoft IT überwacht, und die CPU-Auslastung wird nach dem branchenüblichen P95-Algorithmus gemessen. Bei der Ausführung auf einem relativ großen Server beliefen sich die monatlichen Kosten auf 1.400 Dollar.

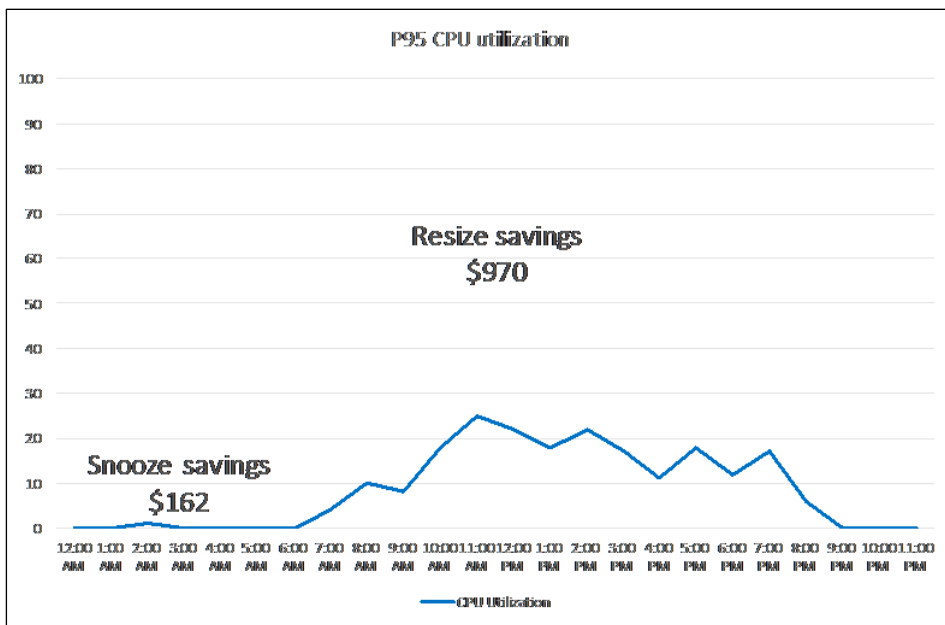


Abbildung 8-4: CPU-Auslastung der IaaS-App

Wie Sie sehen, ist die Anwendung nur zwischen 6 und 21 Uhr aktiv, und die maximale *jemals erreichte* Prozessorauslastung betrug etwa 25 Prozent!

Microsoft IT hat einen „Schlummermodus“ für die Anwendung eingerichtet, um sie außerhalb der Nutzungszeiten vom Netz zu nehmen und die Cloud-Serverressourcen freizugeben. Außerdem wurde die Anwendung auf einen kleineren Server verschoben, der sich besser für die relativ leichte Last eignet.

Mit diesen beiden einfachen Aktionen wurden mehr als Tausend Dollar pro Monat eingespart!

Vergleichen Sie nun diese Kosten mit der lokalen Ausführung der Anwendung: In Ihrem Rechenzentrum bezahlen Sie immer für die Server und können sie nicht einfach in den „Pool“ zurückgeben oder deren Größe ändern. An diesem eindeutigen Beispiel sehen Sie, wie DevOps im Zusammenspiel mit der Cloud beträchtliche Einsparungen ermöglichen kann.

Ein Themenwechsel

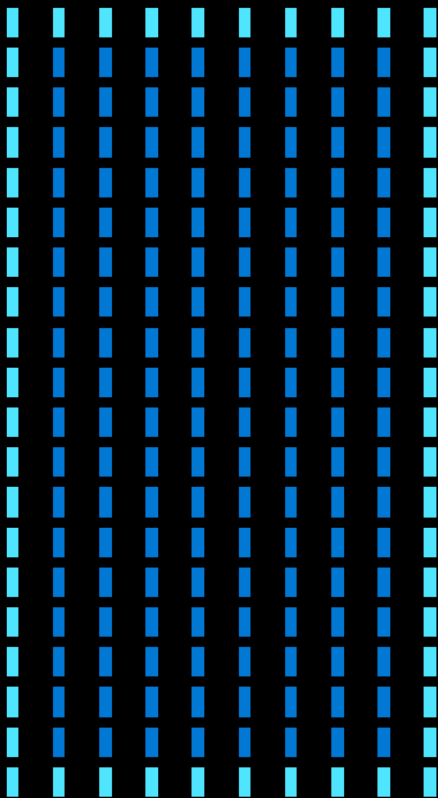
Mit kontinuierlicher Optimierung sind Sie immer auf der Suche nach überdimensionierten Servern, kaum ausgelasteten Datenbanken und Servern und nach Anwendungen, die außerhalb der Nutzungszeiten kaum oder gar nicht verwendet werden. Große IT-Ökosysteme in der Cloud können auf diese Weise buchstäblich Millionen von Dollar einsparen.

Die Optimierung wirkt sich aber auch auf die Gesprächsthemen zwischen IT und deren Geschäftspartnern aus. Ein Lösungseigentümer hat erkannt, dass die Erstellung eines Berichts zu den weltweiten Verkäufen mehr CPU-Leistung benötigt. Darauf folgte ein Geschäftsgespräch: Die Berichte könnten im Unternehmen auf stündlicher Basis zur Verfügung stehen, *wenn Geld für die zusätzlichen Server zur Verfügung stünde*. Wenn ein täglicher Bericht jedoch ausreicht, werden weniger Server benötigt, und die Kosten wären entsprechend niedriger.

Wenn außerdem zu bestimmten Zeiträumen, beispielsweise zum Quartalsende, stündliche Berichte (zu einem Aufpreis) benötigt werden, kann diese Anforderung von der IT umgesetzt werden. Diese Flexibilität ist beispiellos und wäre in einer Welt ohne Cloud nicht möglich gewesen.

Kapitel 9

Sicherheit und Governance in der Cloud



Eine der ersten Fragen, die jeder verantwortliche IT-Leiter stellt, ist die Frage nach der Sicherheit von Anwendungen und Daten in der Cloud.

Die Antwort ist ein klares Ja – sofern die entsprechenden Technologien und Kontrollen eingesetzt werden. Die Gewährleistung der Sicherheit ist ein Bereich, in dem sowohl Technologie als auch Governance eingesetzt werden.

Mit dem Umzug von Anwendungen in die Cloud werden die herkömmlichen IT-Rollen nicht aufgehoben: Sicherheit, korrekte Verwaltung von Unternehmensdaten, Kostenkontrolle und angemessene Verwaltung von Änderungen sind auch weiterhin wichtige Verantwortungsbereiche. Dagegen ändert sich jedoch die Art der Governance von Unternehmen in der Cloud. Dieses Kapitel befasst sich mit Sicherheit und Governance in der Cloud und deren Planung durch IT-Führungskräfte.

Cloud-Sicherheit

Fast jede IT-Führungskraft, mit der wir gesprochen haben, empfand beim Gedanken an den Umzug ihrer IT-Ökosysteme in die Cloud ein gewisses Unbehagen. Immerhin hat die Unternehmens-IT das Ruder in der Hand, wenn sich alle Anwendungen und Daten im lokalen Rechenzentrum befinden. Diese Situation lässt sich mit dem Konzept einer Bank vor 150 Jahren vergleichen. Damals bewahrten die Menschen ihr Bargeld unter der Matratze auf. Schließlich setzte sich jedoch die Erkenntnis durch, dass das Geld in einer Bank von Profis geschützt wird und daher besser aufgehoben ist.

Die Cloud-Sicherheit unterscheidet sich von einer Bank in einem wichtigen Punkt: Die Eigentümer von Anwendungen und Daten müssen aktiv an deren Sicherheit mitwirken. In den nächsten Absätzen umreißen wir einige der Bereiche, denen Sie Aufmerksamkeit und Ressourcen widmen sollten.

Physische Sicherheit

Sicherheit beginnt immer mit der physischen Sicherheit, also der Sicherheit der physischen Einrichtungen, in denen die Cloud ausgeführt wird: die Cloud-Rechenzentren. Cloud-Anbieter tätigen erhebliche Investitionen in die physische Sicherheit und überwachen ihre Einrichtungen rund um die Uhr per Video. Mitarbeiter in Cloud-Rechenzentren werden strengen Überprüfungen unterzogen. Der Zugang zu den Serverbereichen ist nur nach mehreren Authentifizierungen möglich, inklusive einer biometrischen Überprüfung. Alle Aktivitäten werden überwacht und geprüft.

Softwareupdates

Wenn all Ihre Anwendungen auf virtuellen Maschinen (VMs) als Infrastructure-as-a-Service (IaaS) bereitgestellt werden, sind Ihre Mitarbeiter weiterhin dafür verantwortlich, dass Systemupdates und Patches zeitnah installiert werden. Wenn Sie das Plattform-as-a-Service (PaaS)-Modell verwenden, ist Ihr Cloud-Anbieter für die Pflege Ihrer Systemsoftware verantwortlich.

Umfassende Verschlüsselung

Ihre Anwendungen sollten nach Möglichkeit jederzeit Verschlüsselung verwenden. Für Hybrid Cloud verbindungen (zwischen dem lokalen Rechenzentrum und der Cloud) verwenden VPNs und Microsoft Azure ExpressRoute IPSec mit Internet Key Exchange als Transportmethode.

Verwenden Sie nach Möglichkeit Transport Level Security (TLS), die zugrunde liegende Sicherheitstechnologie für HTTP (HTTPS), für den Clientzugriff auf Websites in der Cloud.

Außerdem sollten Sie Ihre ruhenden Daten in Microsoft Azure Speicher oder in Datenbanken ebenfalls immer verschlüsseln, soweit möglich. Eine Azure SQL Database bietet beispielsweise eine Transparent Data Encryption mit einem Serverzertifikat für die Verschlüsselung und Entschlüsselung der Daten in Echtzeit an. Replikate in unterschiedlichen geografischen Regionen verwenden unterschiedliche Zertifikate, die im Normalfall alle 90 Tage ausgetauscht werden.

Schlüsseltresor und Hardwaresicherheitsmodule

Mit einem *Tresor* wie beispielsweise dem Azure Key Vault können Sie die Verschlüsselungsschlüssel separat von der Anwendung aufbewahren. In diesem Fall erstellt ein Administrator zunächst einen Schlüsseltresor für die Anwendung und legt anschließend den oder die Schlüssel in diesem Tresor ab (Abbildung 9-1). Die Entwickler erhalten anschließend vom Azure Key Vault URLs zu den Schlüsseln, die die Anwendung zur Laufzeit zur Entschlüsselung beliebiger Daten verwenden kann, z. B. in Azure Speicher.

Administrator mit Azure
Abonnement erstellt
und verwaltet Tresor
und Schlüssel

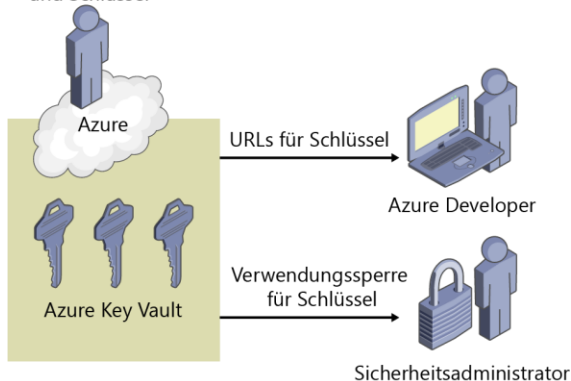


Abbildung 9-1: Azure Key Vault

Um den Schutz zu verbessern, können die Schlüssel in einem Hardwaresicherheitsmodul (HSM) aufbewahrt werden, einem physischen Gerät zum Speichern und Generieren von Schlüsseln. HSMs

können die kryptographische Verarbeitung (normalerweise eine CPU-intensive Aktivität) auslagern und die Daten intern ver- und entschlüsseln.

Antivirensoftware

Das schlimmste, was einer lokalen oder Cloud-Anwendung passieren kann, ist die Entdeckung, dass sie wissentlich oder unwissentlich zur Verbreitung von Viren genutzt wird. Anwendungen (insbesondere IaaS) sollten daher die Vorteile der entweder vom Cloud-Anbieter (z. B. Microsoft Antimalware) oder einem Partner in der Cloud angebotenen Software zum Schutz vor Viren und Schadsoftware nutzen. Alle von dieser Software erkannten Ereignisse werden protokolliert. Cloud-Administratoren sollten diese Log-Dateien in regelmäßigen Abständen untersuchen, um festzustellen, ob Maßnahmen ergriffen werden müssen.

Mehrstufige Authentifizierung

Zur Verbesserung der Sicherheit können Sie einen Multi-Factor Authentication (MFA) für die Benutzeranmeldung verwenden. Bei diesem Verfahren ist neben einem Benutzernamen und einem Kennwort ein zweiter Identitätsnachweis erforderlich, um auf Unternehmensressourcen zuzugreifen. MFA ist in verschiedenen Formen verfügbar, einschließlich biometrischer Modelle, Telefonanrufe und SMS-Nachrichten. Beispielsweise kann bei der Benutzeranmeldung ein Anruf auf ein Mobiltelefon mit Fingerabdrucksensor ausgelöst werden. Die Benutzer können sich erst anmelden, nachdem das Telefon eine gültige Eingabe gemeldet hat.

Eine andere Form der MFA generiert alle paar Sekunden nach einem vorgegebenen Algorithmus eine neue Zufallszahl auf einem mobiles Gerät. Der Benutzer muss die auf dem Telefon angezeigte Zahl eingeben, um Zugang zu erhalten.

Lebenszyklus für die sichere Entwicklung

Obwohl die Cloud zahlreiche Sicherheitsvorteile bietet, werden Anwendungsentwickler und Sicherheitsexperten beim Hosten einer Anwendung in der Cloud nicht von ihrer Verantwortung entbunden. Wir empfehlen Entwicklern und Testern, den Security Development Lifecycle (<https://www.microsoft.com/sdl/default.aspx>) einzuhalten, der mehrere Schritte zum Erkennen und Beseitigen von Bedrohungen umfasst. Antivirus- und Antimalware-Optionen sollten in Ihrer Bereitstellung enthalten sein.

Überwachung von Sicherheitsverletzungen

IT-Führungskräfte sollten ihre Cloud-Anwendungen ebenso wachsam auf Sicherheitsangriffe überwachen wie ihre lokalen Anwendungen. Glücklicherweise stehen bei den Cloud-Anbietern ebenfalls geschulte Sicherheitsexperten zur Verfügung, um die Cloudaktivitäten rund um die Uhr zu überwachen.

Sie können zusätzlich eine Security Intrusion and Event Management (SIEM)-Anwendung bereitstellen, um die Sicherheit weiter zu verbessern. SIEM-Systeme überprüfen Anwendungen auf Schwachstellen, erkennen Angriffe und überwachen das Benutzerverhalten auf Anzeichen für böswillige Aktionen.

Außerdem bietet das Azure Security Center (Abbildung 9-2) den Sicherheitsexperten in Ihrem Unternehmen eine Vielzahl von Funktionen, einschließlich Empfehlungen (z. B. Installation von Patches

oder Aktualisierung der Antivirensoftware), Sicherheitswarnungen (z. B. wenn Ihre Anwendung mit bekannten bössartigen IP-Adressen kommuniziert) und Sicherheitsrichtlinien für Ihre Anwendungen.

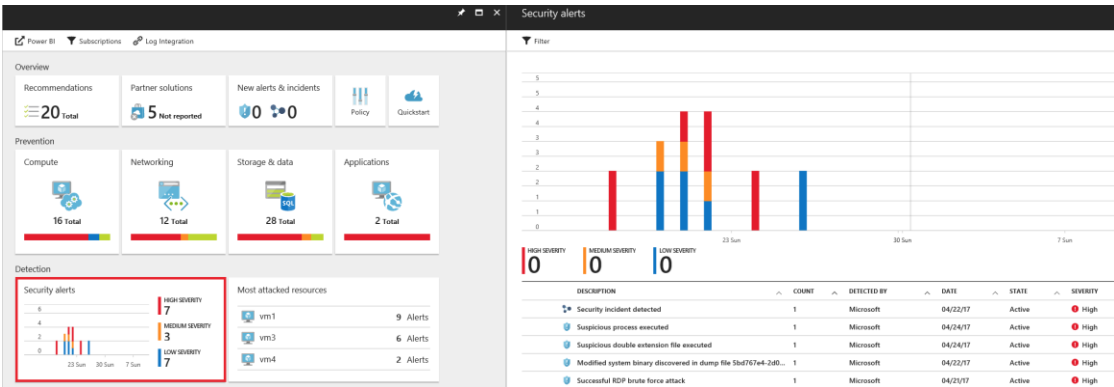


Abbildung 9-2: Azure Security Center

Penetrationstests

Manchmal können Schwachstellen nur gefunden werden, indem Sie tatsächlich versuchen, eine Anwendung zu hacken. Viele Unternehmen beschäftigen Teams von Computersicherheitsexperten, um sogenannte Penetrationstests durchzuführen, eine weithin bewährte Praxis.

Sie sollten jedoch mit Ihrem Cloud-Anbieter zusammenarbeiten, um derartige Tests zu planen, da es ohne vorherige Warnung für den Cloud-Anbieter schwierig ist, zwischen einem Test und einem tatsächlichen Angriff zu unterscheiden.

Verständnis von Cloud-Sicherheitskontrollen

Abbildung 9-3 zeigt die Verteilung von Sicherheitsaufgaben nach Anwendungsmodellen – lokal, IaaS, PaaS und Software-as-a-Service (SaaS).

Lokale Sicherheitsabhängigkeiten	IaaS Infrastructure as a Serv.	PaaS Platform as a Service	SaaS Software as a Service
1. Sicherheitsstrategie, Governance und Operationalisierung: Geben Sie klare Vision, Standards und Orientierungshilfen für die Organisation			
2. Verwaltungskontrolle: Verteidigung gegen den Verlust der Kontrolle über Ihre Cloud-Services und lokale Systeme			
3. Daten: Identifizieren und schützen Sie die wichtigsten Informationen			
4. Benutzeridentität und Gerätesicherheit: Stärkung des Schutzes für Konten und Geräte			
5. Anwendungssicherheit: Stellen Sie sicher, dass der Anwendungscode für Angriffe belastbar ist			
6. Netzwerk: Sicherstellung von Konnektivität, Isolation und Sichtbarkeit in anomale Angriffe			
7. OS and Middleware: Schützen Sie die Integrität der Hosts			
8. Private oder On-Premises-Umgebungen: Sichern der Grundlage			

Abbildung 9-3: Verantwortlichkeiten für Sicherheitskontrollen

Governance, Compliance und Risiko

Unternehmen verfügen schon immer über Mechanismen zur Verwaltung von Governance, Compliance und Risikomanagement. Jedes Unternehmen verwendet Ansätze für den Umgang mit Governance,

Risikomanagement und Compliance, von unorganisierten Ad-hoc-Mechanismen bis hin zu ausgereiften und abgestimmten Praktiken.

Governance, Risikomanagement und Compliance (GRC) sind drei Aspekte, die dazu beitragen, dass ein Unternehmen seine Ziele erfüllt (siehe Abbildung 9-4).



Abbildung 9-4: Framework für Governance, Compliance und Risikomanagement

- Governance ist die Kombination der Prozesse, die von den Direktoren (oder dem Verwaltungsrat) etabliert und zum Erreichen der Ziele verwendet werden.
- Risikomanagement umfasst die Vorhersage, das Verständnis und die Verwaltung von Risiken, die andernfalls das Erreichen der Unternehmensziele beeinträchtigen oder verhindern könnten.
- Compliance bezieht sich auf die Einhaltung von Richtlinien und Verfahren sowie von Gesetzen und Vorschriften.

Die Disziplin GRC zielt darauf ab, Informationen und Aktivitäten für die Bereiche Governance, Risikomanagement und Compliance zu synchronisieren, um effizienter zu arbeiten, einen effektiven Informationsaustausch zu erleichtern, Aktivitätsberichte effektiver zu gestalten und verschwenderische Überschneidungen zu vermeiden.

Jedes GRC-Programm hat daher mindestens die folgenden Ziele:

- Risiken auf einem akzeptablen Niveau halten
- Verfügbarkeit von Systemen und Diensten garantieren
- Relevante Gesetze und Vorschriften einhalten
- Kundendaten schützen

GRC ist in der Regel keine neu für die Cloud eingeführte Funktion, sondern eine Erweiterung vorhandener Aktivitäten. Daher sollten die GRC-Fachkräfte mit den Auswirkungen der Cloud auf ihre jeweiligen Bereiche vollständig vertraut sein und die vorhandenen Methoden ausweiten.

Sicherstellen der Einhaltung gesetzlicher Vorschriften

Die Einhaltung der gesetzlichen Vorschriften kann eine komplexe Aufgabe sein. Für multinationale Unternehmen, insbesondere in stark regulierten Branchen wie Gesundheitswesen und Finanzbranche, ist die Herausforderung unter Umständen noch größer. Die große Anzahl an Normen und Vorschriften ändert sich noch dazu häufig, was es den Unternehmen erschwert, sämtliche internationalen Gesetze zur Datenverarbeitung zu beachten.

Wie auch bei Sicherheitskontrollen müssen die Unternehmen die Aufteilung der Verantwortlichkeiten im Bezug auf die Einhaltung gesetzlicher Bestimmungen in der Cloud verstehen. Cloudanbieter wie Microsoft unternehmen große Anstrengungen, um die Compliance ihrer Plattformen und Dienste zu garantieren. Allerdings müssen die Unternehmen ebenfalls dafür sorgen, dass ihre Anwendungen bzw. die Anwendungen von externen Anbietern ebenfalls compliant sind.

Anwendungen in regulierten Branchen, die Clouddienste verwenden, müssen unter Umständen vom Cloudanbieter zertifiziert werden. Eine Anwendung zur Verarbeitung von Patientendaten im Gesundheitswesen unterliegt beispielsweise den im Health Information Portability and Accountability Act (HIPAA) festgelegten Regeln für Datenschutz und Sicherheit. Unternehmen aus dieser Branche benötigen daher schriftliche Zusagen vom Cloud-Anbieter für den Schutz der empfangenen oder erstellten Patientendaten.

Eine weitere wichtige Bestimmung ist der Payment Card Industry Data Security Standard (PCI DSS), ein proprietärer Informationssicherheitsstandard für Unternehmen, die Kreditkarten der großen Anbieter verarbeiten, darunter Visa, MasterCard, American Express, Discover und JCB. Der PCI-Standard wird von den Kartenanbietern vorgegeben und vom Payment Card Industry Security Standards Council verwaltet. Der Standard wurde geschaffen, um die Kontrolle über die Daten der Karteninhaber zu verbessern und um Kreditkartenbetrug zu reduzieren. Die Einhaltung der Compliance wird jährlich geprüft, entweder durch einen externen qualifizierten Sicherheitsprüfer oder durch einen firmenspezifischen internen Sicherheitsprüfer in Form eines Compliance-Berichts für Unternehmen, die große Transaktionsvolumen verarbeiten, oder durch einen Selbstprüfungsfragebogen für Unternehmen.

Microsoft hat zum aktuellen Datum weit über 50 Compliance-Bescheinigungen erhalten, die Sie in Abbildung 9-5 sehen können. Überprüfen Sie das Azure Trust Center von Zeit zu Zeit, um Updates sowie wichtige Anleitungen zum Thema Compliance zu erhalten.





Global	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> CSA STAR Attestation<input checked="" type="checkbox"/> CSA STAR Certification<input checked="" type="checkbox"/> CSA STAR Self-Assessment	<ul style="list-style-type: none"><input checked="" type="checkbox"/> ISO 22301<input checked="" type="checkbox"/> ISO 27001<input checked="" type="checkbox"/> ISO 27017	<ul style="list-style-type: none"><input checked="" type="checkbox"/> ISO 27018<input checked="" type="checkbox"/> SOC 1 Type 2<input checked="" type="checkbox"/> SOC 2 Type 2
U.S. Government	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> CJIS<input checked="" type="checkbox"/> DoD DISA SRG Level 2<input checked="" type="checkbox"/> DoD DISA SRG Level 4<input checked="" type="checkbox"/> DoD DISA SRG Level 5	<ul style="list-style-type: none"><input checked="" type="checkbox"/> FedRAMP<input checked="" type="checkbox"/> FIPS 140-2<input checked="" type="checkbox"/> High JAB P-ATO<input checked="" type="checkbox"/> IRS 1075	<ul style="list-style-type: none"><input checked="" type="checkbox"/> ITAR<input checked="" type="checkbox"/> Moderate JAB P-ATO<input checked="" type="checkbox"/> Section 508 VPAT<input checked="" type="checkbox"/> SP 800-171
Industry	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> CDSA<input checked="" type="checkbox"/> FACT UK<input checked="" type="checkbox"/> FERPA<input checked="" type="checkbox"/> FFIEC	<ul style="list-style-type: none"><input checked="" type="checkbox"/> FISC Japan<input checked="" type="checkbox"/> GLBA<input checked="" type="checkbox"/> GxP 21 CFR Part 11<input checked="" type="checkbox"/> HIPAA/HITECH<input checked="" type="checkbox"/> HITRUST	<ul style="list-style-type: none"><input checked="" type="checkbox"/> IG Toolkit UK<input checked="" type="checkbox"/> MARS-E<input checked="" type="checkbox"/> MPAA<input checked="" type="checkbox"/> PCI DSS Level 1<input checked="" type="checkbox"/> Shared Assessments
Regional	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> Argentina PDPA<input checked="" type="checkbox"/> Australia IRAP/CCSL<input checked="" type="checkbox"/> Canada Privacy Laws<input checked="" type="checkbox"/> China DJCP<input checked="" type="checkbox"/> China GB 18030<input checked="" type="checkbox"/> China TRUCS	<ul style="list-style-type: none"><input checked="" type="checkbox"/> ENISA IAF<input checked="" type="checkbox"/> EU Model Clauses<input checked="" type="checkbox"/> EU-US Privacy Shield<input checked="" type="checkbox"/> Germany IT Grundschutz<input checked="" type="checkbox"/> India MeitY<input checked="" type="checkbox"/> Japan CS Mark Gold	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Japan My Number Act<input checked="" type="checkbox"/> New Zealand GCIO<input checked="" type="checkbox"/> Singapore MTCS<input checked="" type="checkbox"/> Spain DPA<input checked="" type="checkbox"/> Spain ENS<input checked="" type="checkbox"/> UK G-Cloud

Abbildung 9-5: Microsoft Azure-Compliance-Bescheinigungen

Viele neue Gesetze, insbesondere zu den Themen Privatsphäre und personenbezogene Informationen, schreiben vor, dass die Unternehmen ihre Compliance selbst überwachen und Berichte zur Compliance und zu aufgetretenen Problemen erstellen.

Eine der wichtigsten Entwicklungen in diesem Bereich ist die jüngste Verordnung der Europäischen Kommission im Rahmen der EU-Datenschutz-Grundverordnung (DSGVO) zur Stärkung des Datenschutzes für Personen in der Europäischen Union. Die DSGVO schreibt vor, dass Daten über Einzelpersonen (Name, Adresse, Foto, E-Mail-Adresse, Bankverbindung, Beiträge auf Social Networking-Websites, medizinische Informationen oder IP-Adressen von Computern)¹¹ auf Servern innerhalb der EU aufbewahrt werden müssen und diese nicht verlassen dürfen. Außerdem müssen Unternehmen Einzelpersonen über sämtliche Datenschutzverletzungen benachrichtigen und einen Datenschutzbeauftragten ernennen. Andere Länder haben ähnliche Verordnungen oder sind dabei, diese zu entwickeln.

Azure bietet eine Reihe von Diensten an, die Sie bei der Einhaltung der DSGVO und ähnlichen Initiativen (Abbildung 9-6) unterstützen. Azure Information Protection bietet Dokumentüberwachung und Widerrufsfähigkeiten, mit denen Sie nicht nur den Fluss der Daten im Unternehmen überwachen, sondern auch den Zugriff widerrufen können. Mit Microsoft Office 365 Advanced Data Governance können Sie Unternehmensdaten klassifizieren.

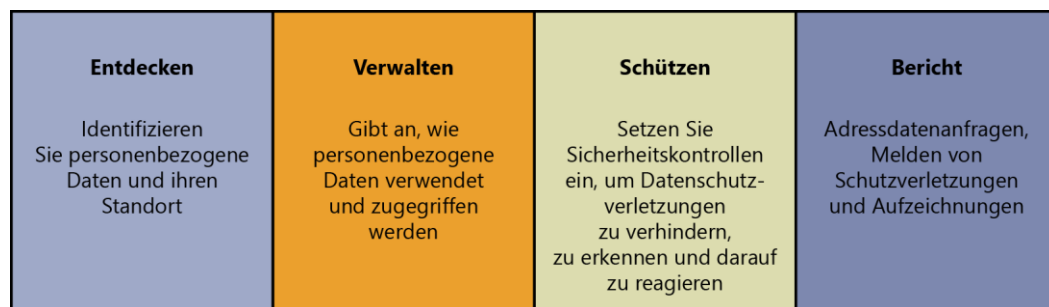
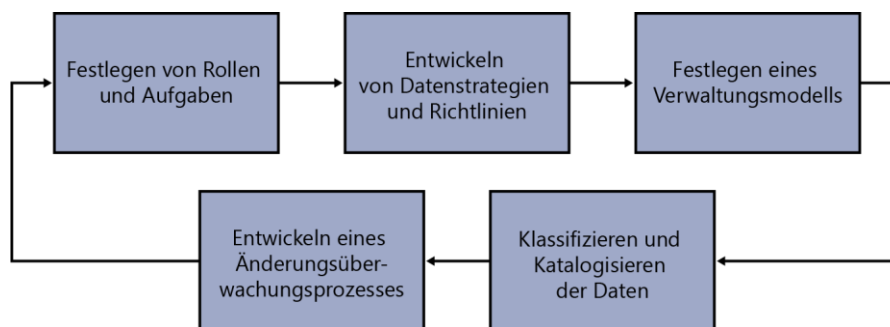


Abbildung 9-6: Einhaltung der DSGVO und anderer Initiativen

Data Governance

Eine Data Governance-Funktion ist unerlässlich für die Einhaltung vieler Vorschriften und Normen. Data-Governance im IT-Bereich war schon lange vor der Cloud eine kritische Funktion. Erstellung und Einhaltung häufig verwendeter Datenmodelle, Erweiterbarkeit bei Bedarf, Änderungsverwaltung, regelmäßige und gesteuerte Taxonomieaktualisierungen, Festlegen der Verwendung von Master- und Referenzdaten, Implementieren einer Datenklassifizierung, Einrichten formaler Prozesse zur Beibehaltung und Löschung von Daten: All dies ist schon seit Jahrzehnten Teil der IT Governance. Abbildung 9-7 zeigt die an der Data Governance beteiligten Prozesse.



¹¹ http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

Abbildung 9-7: Data Governance-Prozess

Machen Sie sich bewusst, welche Daten Ihre Anwendungen in der Cloud aufbewahren und welche Gesetze in Ihrem Land oder Ihrer Region hinsichtlich der Datenhoheit und der Verschiebung von Daten über Grenzen hinweg gelten. Dazu bietet sich unter anderem die Implementierung der folgenden Maßnahmen an:

- Speichern Sie keine personen- oder kundenbezogenen Daten in der Cloud.
- Verschlüsseln Sie wichtige personenbezogene Daten wie E-Mail-Adressen oder Anschriften, bevor Sie die Daten in die Cloud verschieben.
- Deaktivieren Sie die Georeplikation für andere Standorte.

Financial Governance

Die wichtigsten Änderungen, die sich im Rahmen der Cloud-Umstellung für die IT-Finzen ergeben haben, wurden bereits beschrieben: der Übergang vom Kapitalkostenmodell zum Betriebskosten- oder Abonnementmodell. Financial Governance stellt dabei sicher, dass die finanziellen Änderungen systematisch und planbar verwaltet werden. Dies umfasst Folgendes:

- Die tatsächlichen Kosten für die Cloud stimmen mit den vorgesehenen Kosten überein.
- Die Kapitalkosten verringern sich wie vorgesehen.
- Abonnements werden in zumutbarer Weise (z. B. nach Kostenstelle oder Einsatzgebiet) verwaltet, und nicht autorisierte Kreditkartenkonten sind nicht zulässig.
- Entsprechende Rückbelastungssysteme werden erstellt oder für den Support von Cloud Computing ausgeweitet.
- Quartals- oder Jahresbudgets zeigen die entsprechenden Änderungen an.
- Berichtssysteme zeigen die aktuellen IT-Ausgaben exakt an.

Änderungsverwaltung

Die meisten IT-Organisationen verfügen über ein Programmmanagementbüro. Dessen Aufgaben bestehen darin, sicherzustellen, dass Änderungen mit minimalen Risiken und Funktionsunterbrechungen der IT abgewickelt werden. Beim Umstieg müssen die neuen Änderungsverwaltungsfunktionen verwaltet werden. Dazu gehört Folgendes:

- Betriebliche Bereitschaft, um sicherzustellen, dass der Betrieb oder die DevOps-Funktion zur Verwaltung einer Cloudanwendung bereit ist
- Bereitschaft der Benutzer im Falle funktionaler Änderungen bei Anwendungen
- Bereitschaft der Organisation, um beispielsweise sicherzustellen, dass abhängige Anwendungen weiterhin funktionieren und alle Sicherheits-, Compliance- und Finanzanforderungen erfüllt sind
- Bereitschaft der Anwendung und des Ökosystems, um sicherzustellen, dass die Anwendungen, die Umstieg auf die Cloud werden, sowie die Anwendungen, die bleiben und in Cloudanwendungen integriert werden, vollständig getestet und bereit sind und dass alle Probleme im Voraus bekannt sind.

Governance umfasst noch weitere Aspekte (z. B. Lieferantenmanagement). Nun sollte jedoch klargeworden sein, dass Governance in der Cloud im Großen und Ganzen vorhandene Funktionen ausweitet, und Fachkräfte in diesen Bereichen sollten die Auswirkungen von Cloudanwendungen in ihrem Bereich berücksichtigen.

ITIL und die Cloud

In Kapitel 8 haben Sie gesehen, dass Unternehmen die Implementierung neuer Features in ihren Cloud-Anwendungen mit einem DevOps-Modell der kontinuierlichen Integration und Bereitstellung deutlich beschleunigen können. Für viele Anwendungen müssen die Änderungen jedoch streng kontrolliert werden, z. B. Anwendungen zur Verwaltung der Unternehmensfinanzen. Das offensichtlichste Beispiel in diesem Bereich sind Enterprise Resource Planning (ERP)-Systeme. Die Nachfrage nach diesen herkömmlichen Frameworks zur Kontrolle von Änderungen und den Folgerisiken bleibt auch in Zukunft erhalten.

Viele IT-Organisationen verwenden das ITIL-Framework für die Dienstverwaltung und den Betrieb. Im Laufe der Jahre hat sich ITIL¹² bei der IT-Dienstverwaltung (IT Service Management, ITSM) sowie zum Ausrichten der IT-Investitionen und des Betriebs an die Ziele des Unternehmens bewährt. Größere Zuverlässigkeit, Betriebszeiten und vorhersehbare Kosten werden häufig als Vorteile von ITIL genannt.

ITIL betrifft die *IT-Dienste*, d. h. die Funktionen und Prozesse, die IT-Organisationen den Unternehmen bereitstellen. Ein Dienst – etwa eine Anwendung, eine Reihe von Anwendungen, Informationen, Personen – wird von einem Unternehmensbenutzer zum Ausführen einer Unternehmensfunktion genutzt. Im Allgemeinen ändern sich die Ziele von ITIL durch die Cloud-Technologie nicht, die Cloud kann, wie gezeigt, die Bereitstellung von Diensten jedoch grundlegend ändern.

ITIL besteht aus fünf zentralen strategischen Bereichen:

IT-Servicestrategie Die ITIL-Servicestrategie umfasst diverse Frameworks, um festzulegen, welche Dienste bereitgestellt werden, wie ihr Wert gemessen wird und wie Kosten gemessen werden. Zudem bieten sie einen Maßstab für die Return-on-Investment (ROI) und legen fest, wie die IT-Beziehung zu Unternehmenspartnern verwaltet wird. Am Anfang dieses Kapitels wurde beschrieben, wie eine Strategie eingerichtet wird, die die gesamten (technischen, finanziellen und unternehmensbezogenen) Ziele der Cloud-Migration definieren.

- **IT-Serviceentwicklung** Dieser Bereich umfasst die Gestaltung von Prozessen und deren Beziehung zueinander, Vereinbarungen zum Servicelevel (SLA), Kapazitäts- und Verfügbarkeitsverwaltung, Business-Continuity verwaltung, Sicherheit und Lieferantenmanagement. Einige dieser Themen wurden in diesem Kapitel bereits besprochen, und Muster für Sicherungen und Business-Continuity finden Sie in Anhang B.

Bei der IT-Serviceentwicklung ist auch ein Dienstkatalog erforderlich, der zum wesentlichen Teil aus Portfolio- und Konfigurationsverwaltungssystemen besteht.

- **IT-Serviceinbetriebnahme** Die Serviceinbetriebnahme legt fest, wie Dienste bereitgestellt werden. Bereiche wie Änderungs-, Release- und Bereitstellungsverwaltung sowie Dienstevaluierung gehören in der Regel zur Inbetriebnahme. Das Ziel besteht natürlich darin, neue Dienste sowie Änderungen an bestehenden Diensten mit minimalen Auswirkungen auf das gesamte IT-Ökosystem bereitzustellen.

Obwohl die Struktur bei der Serviceinbetriebnahme gleich bleibt, ändern sich die Aufgaben bei der Bereitstellung eines Diensts für die Cloud wie bereits beschrieben stark. Insbesondere die Entstehung von DevOps und der dazugehörigen Methoden hat zu einem Wandel der mit der

¹² ITIL® ist eine eingetragene Marke der UK Cabinet Office.

Bereitstellung verbundenen Prozesse und Tools geführt. Außerdem sollten IT-Abteilungen verschiedene Bereiche überdenken, z. B. die Messung der SLA-Einhaltung. Beispielsweise kann es passieren, dass der Datenverkehr über das offene Internet bis zur Cloud zusätzlicher Latenz unterliegt.

Dementsprechend müssen IT-Abteilungen eine Testcloud-Umgebung einrichten, die die Produktionsumgebung abbildet, um Benutzerakzeptanztests (User Acceptance Testing, UAT), Last- und Penetrationstests sowie Integrationstests mit anderen Anwendungen vor einer vollständigen Produktionsbereitstellung zu ermöglichen.

- **IT-Servicebetrieb** Die Dienstverwaltung umfasst auch die Verwaltung und Überwachung von Diensten sowie Problemverwaltung und -lösung. Ein zentrales Konzept der Dienstverwaltung besteht im Service Desk, der ersten Anlaufstelle für Dienstvorfälle und -ereignisse. Der Service Desk muss, wie auch das Callcenter und der Helpdesk (sofern diese separat sind), für cloudbasierte Dienste geschult werden.
- **Kontinuierliche IT-Serviceverbesserung** Bei der kontinuierlichen Serviceverbesserung (CSI) arbeiten IT-Fachkräfte und Unternehmensteams zusammen, um sicherzustellen, dass die Dienste neue und aufkommende Geschäftsanforderungen erfüllen. CSI ist stark datenorientiert und basiert auf Vorgangstatistiken sowie auf Geschäftserkenntnissen, um festzustellen, worauf der Fokus liegen sollte.

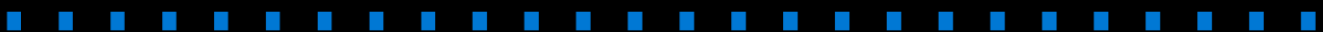
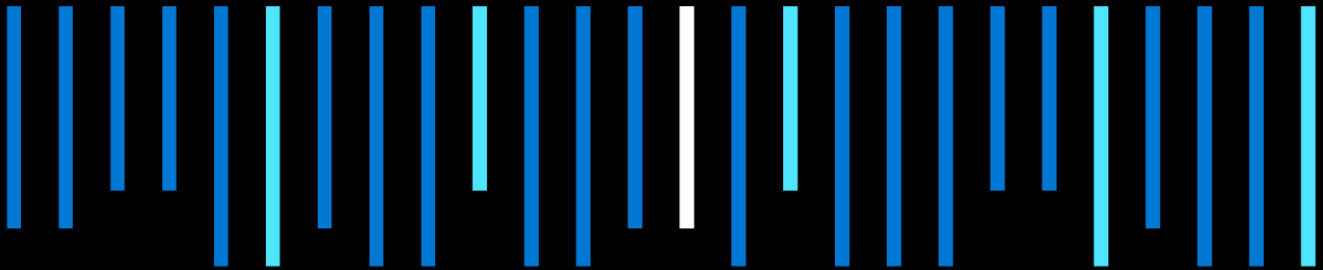
Im Allgemeinen müssen Unternehmen bei der Cloud-Migration einige Mechanismen und Prozesse zur ITIL-Implementierung ändern, auch wenn die grundlegende Struktur von ITIL in der Regel technologieunabhängig ist. Organisationen sollten jedoch auch überlegen, wie sie ihre Prozesse ausweiten können, um agiler zu werden, als es durch ITIL möglich zu sein scheint. Da das Testen und Erstellen von Prototypen schnell abläuft, sind diese als Teil der Strategie und der ITIL-Designphasen anzusehen.

Der Umzug von Anwendungen zur Cloud ist eine wichtige Aufgabe, die Änderungen an der Arbeitsweise sowohl von Unternehmen als auch der IT erfordert. In Teil II wurde beschrieben, wie ein Cloud-Strategieteam für die Migration gebildet und eingesetzt wird, wie die Beteiligten in einer Organisation einbezogen werden, welche Prioritäten bei der Anwendungsmigration gelten und wie bestehende Governance-Aktivitäten ausgeweitet werden.

Die Aspekte, die sich auf die Transformation beziehen, sind beim Wechsel zur Cloud ebenso von Bedeutung und sollten parallel zur Migration untersucht und umgesetzt werden. Die transformative Innovation und die Möglichkeiten, die sich durch die Cloud bieten, sind in Teil III beschrieben.

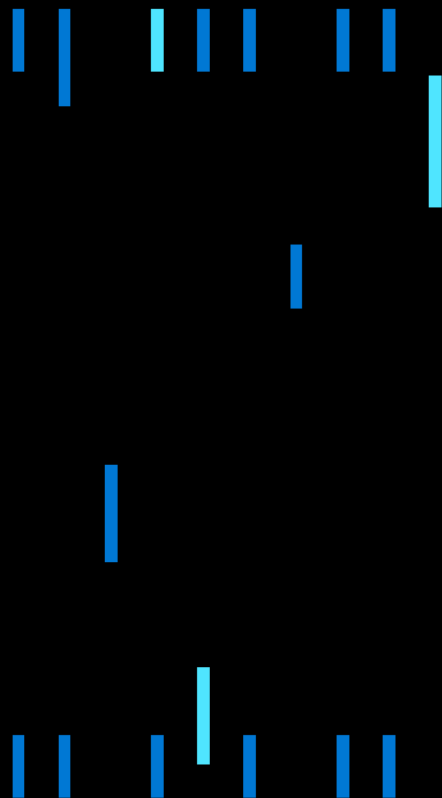
Teil III

Ein neues IT-Zeitalter



Kapitel 10

In die Cloud und wieder zurück



Obwohl sich ein Großteil dieses Buchs auf den Umzug ganzer Anwendungen und Ökosysteme in die Cloud konzentriert, können auch lokale Computing-Ressourcen mit Cloud-Technologien effizienter und kostengünstiger eingesetzt werden. Viele der eher banalen IT-Aufgaben wie Backup und Wiederherstellung können in und aus der Cloud sicher und kostengünstig durchgeführt werden. Mit Messaging Bus- und Integration Broker-Systemen können sich Unternehmen mühelos mit Business-to-Business (B2B)-Websites verbinden. Außerdem können sie ihre Unternehmensverzeichnisse in die Cloud erweitern, um ihre sichere Identitätsverwaltung auf Cloud-Ressourcen auszuweiten. Im Laufe der Zeit kann es auch Sinn machen, bestimmte Cloud Computing-Paradigmen wieder zurück in das Rechenzentrum zu spiegeln.

Sicherung und Wiederherstellung

Eine der unscheinbarsten und dennoch wichtigsten Aufgaben einer IT-Abteilung besteht darin, sicherzustellen, dass die Unternehmensdaten auch nach Serverabstürzen, Stromausfällen, versehentlichen Datenlöschungen und ähnlichen Vorfällen niemals verloren gehen. In der Vergangenheit bestanden Sicherungen normalerweise darin, den Inhalt mitten in der Nacht von Laufwerken auf ein Offlinemedium (z. B. ein Band) zu kopieren und diese Bänder anschließend an einem separaten Standort aufzubewahren.

Die Cloud ermöglicht einen neuen Sicherungsansatz für lokale und Cloud-Anwendungen. Der Grund ist leicht zu erkennen: Die enormen Kapazitäten an kostengünstigem Speicher mit integrierter Sicherheit und Cloud-Rechenzentren auf der ganzen Welt sind herkömmlichen Sicherungslösungen ebenbürtig oder übertreffen diese sogar.

Beachten Sie zwei wichtige Metriken bei der Erarbeitung eines Plans für Ihre Sicherungsstrategie:

- **Recovery Time Objective (RTO):** Wie schnell müssen Sie Ihre Daten wiederbekommen?
- **Recovery Point Objective (RPO)** Wie aktuell müssen die Daten nach der Wiederherstellung sein? (In anderen Worten, wie häufig müssen Sie sichern? Täglich? Stündlich?)

Es gibt viele Cloud-Lösungen für Sicherung und Wiederherstellung, jeder zielt auf eine bestimmte Workload oder ein bestimmtes Szenario ausgerichtet sind. Microsoft Azure Backup sichert, wie der Name bereits andeutet, Daten in einem Cloud-Speicher. Die Daten werden mit AES-256 verschlüsselt, mit bis zu sechs separaten Kopien in zwei separaten Rechenzentrums-Regionen (wenn Sie die Georedundanzoption auswählen, sind die Rechenzentren mindestens 160 Kilometer voneinander entfernt). Wie alle Cloud-Komponenten ist auch Azure Backup ein Prepaid-Service: Sie bezahlen nur für die tatsächlich genutzten Ressourcen.

Achten Sie auch auf die *Sicherungsmethode*. Wie Sie in Abbildung 10-1 sehen, können Sie in modernen Sicherungstechnologien (darunter auch Azure Backup) entweder ein *vollständiges Backup* auswählen, bei dem die gesamten Quelldaten kopiert werden, ein *differenzielles Backup*, bei dem nur die Datenblöcke gesichert werden, die seit dem *ersten vollständigen Backup* geändert wurden, oder ein *inkrementelles Backup*, bei der nur Daten gesichert werden, die seit dem *vorherigen Backup* geändert wurden. Am effektivsten ist natürlich zunächst eine vollständige Sicherung, gefolgt von regelmäßigen inkrementellen Sicherungen.

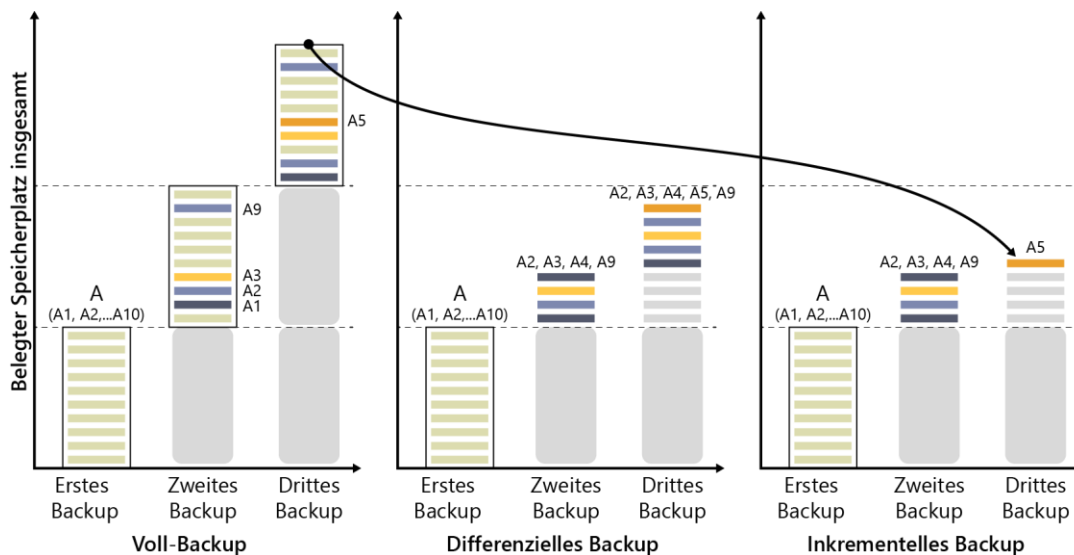


Abbildung 10-1: Backup-Modi

Sie müssen selbst auswählen, welches Intervall und welcher Sicherungstyp am besten für Ihre Anforderungen und für Ihre RTO- und RPO-Ziele geeignet sind. Mit Azure Backup sind Ihre Anwendungsdaten immer *konsistent* und daher für beliebige RPO-Ziele immer in einem nutzbaren Zustand.

Wenn Sie die Microsoft Systemverwaltungstools (Microsoft System Center) bereits in Ihrem Unternehmen installiert haben, können Sie die Data Protection Manager erweitern, um Ihre Daten in der Cloud zu sichern. Data Protection Manager ist eine voll funktionsfähige Lösung für Sicherungen auf Band, auf anderen Medien oder in der Cloud, in dieselben „Datentresore“, die auch Azure Backup verwendet. Außerdem können Sie Transact-SQL verwenden, um Microsoft SQL Server für die Sicherung von Daten in der Cloud konfigurieren.

Lokalen Speicher in die Cloud erweitern

IT-Führungskräfte müssen aufgrund von gesetzlichen Bestimmungen oft riesige Mengen an Verlaufsdaten aufbewahren. Auf diese Daten wird normalerweise sehr selten zugegriffen (oft im Zusammenhang mit gesetzlichen Anforderungen), aber die Daten müssen laut Gesetz verfügbar sein.

Für diese Fälle ist eine Speichereinrichtung hilfreich, die zwar lokal eingerichtet wird, aber die Cloud-Umgebung kennt. Wenn der Speicherplatz knapp wird, kann eine solche Einrichtung die selten verwendeten Daten in die Cloud auslagern. Auf diese Weise sind die Daten weiterhin lokal verfügbar, aber das Gerät kennt den Speicherort des gesamten Datenvolumens, um die Daten im Fall einer gesetzlichen Anforderung schnell wiederherstellen zu können. Microsoft bietet mit der StorSimple-Appliance eine solche Lösung an.

Business-Continuity und Notfallwiederherstellung

Ein CIO hat mir einmal von einem Rechenzentrum in seinem Unternehmen erzählt, in dem eine nicht geerdete Antenne auf dem Dach stand. Einige Zeit später schlug ein Blitz im Rechenzentrum in genau diese Antenne ein und verursachte einen katastrophalen Ausfall sämtlicher Systeme. IT-Führungskräfte bemühen sich zwar, solche Katastrophen zu vermeiden. Allerdings geschehen sie dennoch, und die IT muss vorbereitet sein.

Eine optimale Business Continuity und Disaster Recovery (BC/DR)-Lösung führt einen nahtlosen *Failover* von dem ausgefallenen Standort auf ein anderes Replikat durch, auf dem dieselbe Software mit aktuellen Daten ausgeführt wird. Wie auch bei der einfachen Sicherung gelten die Konzepte von RTO und RPO auch für BC/DR, und IT-Führungskräfte sollten ihre Ziele für diese Metriken im Rahmen einer BC/DR-Gesamtstrategie aufstellen. Außerdem sollten Sie Ihre BC/DR-Failoverlösung regelmäßig (monatlich oder einmal pro Quartal) *testen*, und Ihre BC/DR-Lösung sollte diese Tests ohne Unterbrechungen am Tagesgeschäft unterstützen.

Wenn der ausgefallene Standort wiederhergestellt wurde, müssen Sie die *Reihenfolge* kontrollieren, in der die Anwendungen wieder online geschaltet werden, da diese häufig voneinander abhängen.

Mit Azure Site Recovery können Sie eine vollständige BC/DR-Lösung in der Cloud implementieren, volle Datenkonsistenz gewährleisten, Tests ohne Unterbrechungen durchführen und maßgeschneiderte Wiederherstellungspläne erstellen.

Integration

Wie bereits erwähnt wird es immer eine Übergangszeit geben, in der ein Teil Ihrer Anwendungen in Ihrem Rechenzentrum verbleibt, während andere Anwendungen in die Cloud umgezogen wurden. Dies gilt auch, wenn Sie Ihr gesamtes Anwendungsportfolio von lokalen Ressourcen in die Cloud umziehen. Höchstwahrscheinlich werden Sie sich jedoch entschließen, einen Teil Ihrer Anwendungen für die absehbare Zukunft im lokalen Rechenzentrum zu behalten: ein sogenanntes Hybrid Cloud-Modell.

In beiden Fällen muss das Anwendungsportfolio des Unternehmens so integriert werden, dass sämtliche Anwendungen weiterhin wie gehabt funktionieren, als ob sie sich im gleichen Netzwerk befänden, und mit minimalen oder keinen Änderungen am Benutzererlebnis. In den folgenden Abschnitten beschreiben wir einige Ansätze, mit denen Sie diese Integration gewährleisten können.

Netzwerk

Zunächst sollten Sie sicherstellen, dass cloudbasierte Anwendungen für das Unternehmensnetzwerk sichtbar sind, sich also im entsprechenden Subnetz befinden. Sie erreichen dies durch den Einsatz eines Virtual Private Network (VPN) oder durch die Implementierung einer physischen Standleitung, die das Rechenzentrum des Unternehmens mit dem Cloud-Rechenzentrum verbindet.

VPN-Optionen

IT-Abteilungen können VPNs entweder nur per Software verbinden (*Punkt-zu-Standort*) oder mit einem VPN-Hardwaregerät (*Standort-zu-Standort*). In Punkt-zu-Standort-Konfigurationen ist nur ein lokaler Computer mit den Cloud-Ressourcen verbunden. Dieses Szenario macht Sinn für Benutzer, die sich beispielsweise von Zuhause oder von einer Konferenz aus verbinden.

In Standort-zu-Standort-Konfigurationen erstellt ein spezielles VPN-Hardwaregerät einen verschlüsselten (IPSec, mit Internet Key Exchange [IKE]) Tunnel zwischen dem Rechenzentrum und der Cloud. Die IP-Adressen werden im Gerät so konfiguriert, dass die Cloud-Ressourcen scheinbar im lokalen Netzwerk befinden (siehe Abbildung 10-2).

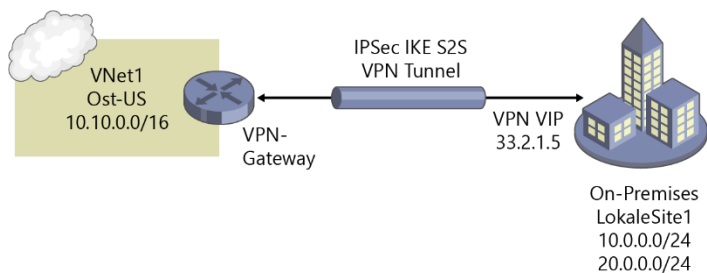


Abbildung 10-2: Hardware-VPN

VPNs dieser Art können in mehreren lokalen Rechenzentren eingerichtet werden (siehe Abbildung 10-3):

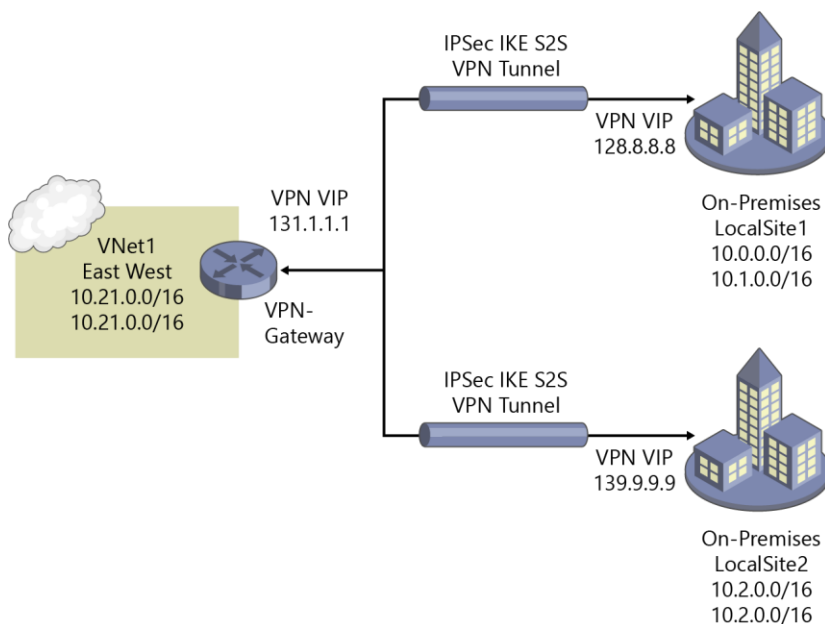


Abbildung 10-3: Standortübergreifende VPN-Verbindungen

Azure ExpressRoute

Mit einer Standleitung wie Azure ExpressRoute können Unternehmen ihren Standort direkt mit der Cloud verbinden. Allerdings müssen die Standleitungen vom lokalen Telekommunikationsanbieter erworben werden, und Sie müssen die entsprechenden Edge-Router und andere Hardware vor Ort installieren. Abbildung 10-4 zeigt einen Überblick über eine ExpressRoute-Konfiguration.

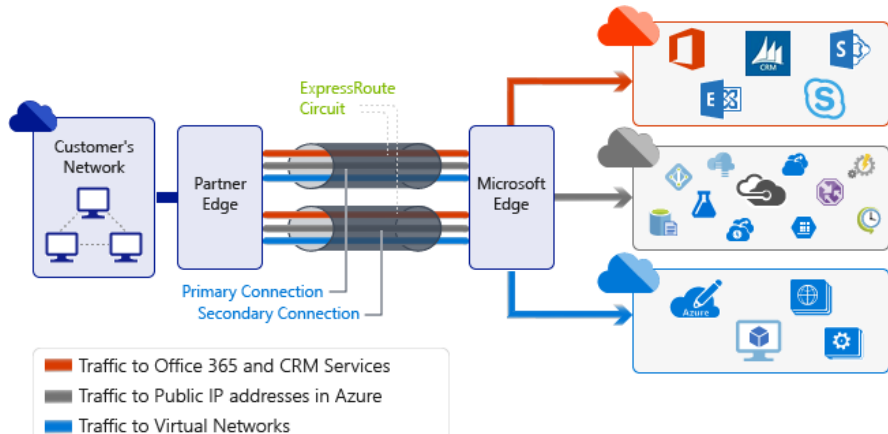


Abbildung 10-4: ExpressRoute

Diese Standleitungen bieten die folgenden Vorteile:

- Sie können in der Regel eine garantierte Bandbreite von Ihrem Telekommunikationsanbieter erwerben.

Sie können ExpressRoute verwenden, um sich mit beliebigen Cloud-Diensten von Microsoft zu verbinden.

Die Nachrichten werden nicht über das öffentliche Internet übertragen, was die Sicherheit verbessert.

Für Standleitungen wie ExpressRoute fallen jedoch zusätzliche Kosten an, je nach der gewünschten Bandbreite, den vom ausgewählten Telekommunikationsanbieter festgelegten Preisen usw.

Messaging: Service Bus

Die Cloud ermöglicht verschiedene Ansätze für die Integration von Anwendungen. Azure Service Bus kann Verbindungen zwischen reinen Cloud-Anwendungen oder zwischen lokalen und Cloud-Anwendungen herstellen und ermöglicht zahlreiche verschiedene Architekturoptionen für den Nachrichtenaustausch zwischen Anwendungen. Der Service Bus ist ein zuverlässiger Dienst für die Informationsübertragung, ähnlich einem echten Postamt.

Unter anderem werden die folgenden Methoden für die Nachrichtenzustellung unterstützt:

- **Warteschlangen** Für First-in, First-out-Messaging
- **Themen und Abonnements** Anwendungen können einen Typ zu bestimmten Nachrichten zuweisen, damit diese von anderen Anwendungen abonniert werden können

Azure Service Bus ist ein extrem sicherer Allzwecknachrichtenbroker und sorgt dafür, dass die Nachrichten zuverlässig zugestellt werden. Alle Aktionen sind *transaktional*, d. h. wenn eine bestimmte Aktion (z. B. Zustellung) nicht abgeschlossen werden kann, wird sie in einen bekannten konsistenten Zustand zurückversetzt.

Serverlose Anwendungsintegration: Logic Apps

Auf der höchsten Ebene der Anwendungsintegration befinden sich Broker, die B2B-Protokolle direkt umsetzen und auch verwendet werden können, um benutzerdefinierte Enterprise-Workflows einzurichten.

Der einfachste Weg für dieses Modell sind sogenannte Integration-Platform-as-a-Service (iPaaS)-Broker, allen voran die Microsoft Azure Logic Apps.

Mit Logic Apps können Unternehmensentwickler ihre Anwendungen mit Branchenprotokollen und ohne Code vernetzen. Dieses sogenannte „serverlose“ Konzept wird in Kapitel 11 ausführlich besprochen. Connectoren für Logik-Apps umfassen EDI X.12, HL7 FHIR, XML, SMS, SAP und Hunderte weiterer Anbieter. Die Logic Apps benötigen keinen Code und ermöglichen daher eine schnelle und zuverlässige Anwendungsintegration.

Erweitern von Verzeichnisdiensten in die Cloud

Für die Identitätsverwaltung in Unternehmen gelten die drei folgenden wichtigen Ziele:

- Die Benutzer melden sich per „Single Sign-On“ (SSO) bei den Anwendungen an, sowohl im Rechenzentrum als auch in der Cloud.
- Die Benutzer müssen sich von außerhalb des Unternehmensnetzwerks bei Anwendungen anmelden können, beispielsweise um von Zuhause aus arbeiten zu können.
- Für bestimmte Anwendungen wird möglicherweise eine Authentifizierung über externe Anbieter (z. B. Microsoft-Konto, Facebook oder Google-Anmeldeinformationen) erlaubt, unter Umständen mit eingeschränkten Berechtigungen.

Um diese Ziele zu erreichen, sollten Unternehmen ihre Verzeichnisdienste in die Cloud erweitern, zum Beispiel mit Azure Active Directory (Azure AD), wie in Abbildung 10-5 gezeigt.

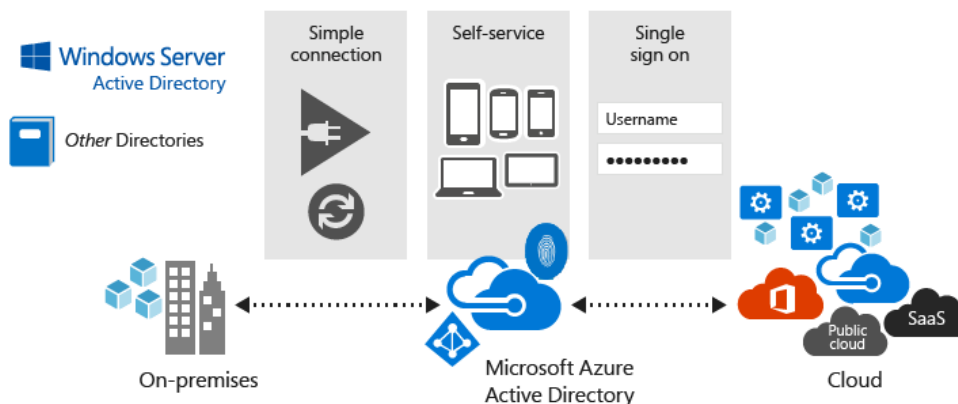


Abbildung 10-5: Azure Active Directory

Azure AD synchronisiert sich mit lokalen Verzeichnissen wie Windows Server Active Directory und anderen. Auf diese Weise können sich die Benutzer einmal anmelden und erhalten Zugriff auf alle Anwendungen im Rechenzentrum und in der Cloud. Außerdem können sich die Benutzer von außerhalb des Rechenzentrums anmelden, und Azure AD verwaltet den Authentifizierungsprozess in Abstimmung mit dem lokalen Verzeichnis. Außerdem kann Azure AD Authentifizierungsquellen aus dem Internet verwalten, darunter Facebook- und Microsoft-Konten.

Einer der wichtigsten Aspekte von Azure AD ist sind die Connectoren für führende Software-as-a-Service-Anwendungen. Die Benutzer melden sich nur einmal an und erhalten neben den Unternehmensanwendungen auch Zugriff auf andere Anwendungen wie Microsoft Office 365, Salesforce.com, Dropbox, Concur und viele andere.

Mit Azure AD erhalten Sie außerdem die Tools, um die Authentifizierung von Verbrauchern im großen Stil zu implementieren, beispielsweise für eine E-Commerce-Website, die ihre Kunden authentifizieren muss.

Cloud Computing in Ihrem Rechenzentrum

Wenn Sie Ihre Anwendungen in die Cloud umziehen und in manchen Fällen möglicherweise umgestalten, gelangen Sie irgendwann an den Punkt, an dem sich Ihre Mitarbeiter besser mit Cloudtechnologien auskennen als mit den herkömmlichen lokalen Modellen. Möglicherweise benötigen Sie auch eine absolut deterministische Latenz für Ihre Cloud-Anwendungen, d. h. manche Anwendungen vertragen die schwankenden Antwortzeiten bei der Übertragung über das offene Internet nicht (ein Beispiel sind Fertigungsgeräte an einem Fließband). In anderen Fällen kann es vorkommen, dass die Verbindung zur Cloud nicht garantiert werden kann.

Für diese zugegebenermaßen seltenen Anwendungstypen kann es Sinn machen, ein „Cloud-Gerät“ einzusetzen, also einen Server, auf dem die Cloud-Software ausgeführt wird. Ein Beispiel hierfür ist Azure Stack. Azure Stack besteht aus Cloud-Softwarepaketen, die auf ausgewählten Serverplattformen ausgeführt werden können.

Durch die Ausführung von Cloud-Diensten in Ihrem Rechenzentrum können Sie Latenzen wie in einem lokalen Netzwerk garantieren. Wenn Sie beispielsweise Fertigungsgeräte einsetzen, die minimale Antwortzeiten benötigen, können Sie Azure Stack lokal installieren, um die vom offenen Internet verursachten Latenzschwankungen zu eliminieren. Abbildung 10-6 zeigt einen Übersicht über Azure Stack.

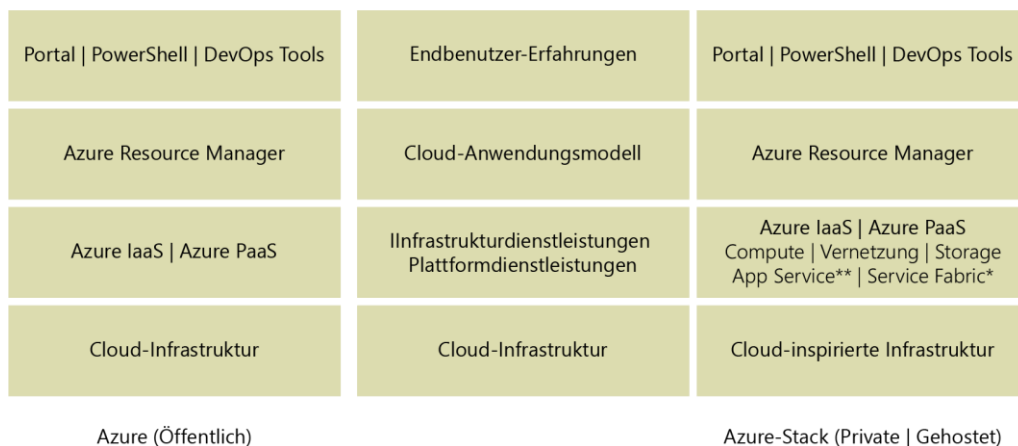


Abbildung 10-6: Azure Stack

Wenn Sie die Internetverbindung nicht garantieren können, ist Azure Stack eine Möglichkeit, um die Verfügbarkeit Ihrer Dienste sicherzustellen, selbst wenn Ihre Internetverbindung inaktiv oder nicht verfügbar ist. Ein großes Kreuzfahrtunternehmen setzt beispielsweise Azure Stack ein, um dieses Problem zu lösen.

Mit Azure Stack können Sie eine PaaS-Anwendung oder eine serverlose Funktion einmal für die Cloud entwickeln und anschließend entweder in der Cloud oder lokal bereitstellen, damit Ihre Entwicklungsteams ein einziges Programmierungsmodell verwenden können.

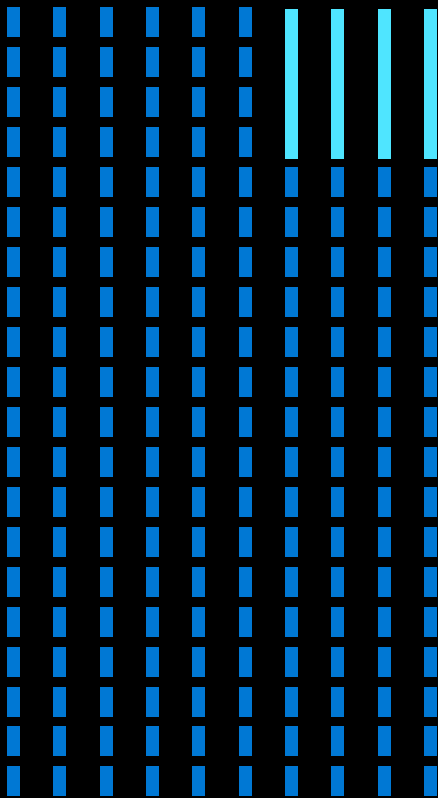
Verwaltung von Hybrid Clouds

Die Verwaltung verschiedener Anwendungen in unterschiedlichen Rechenzentren und in der Public Cloud ist eine Herausforderung. Eine Lösung zur Verwaltung all dieser Anwendungen muss in der Lage sein, Grenzen zwischen Betriebssystemen und Rechenzentren zu überschreiten und Administratoren eine konsolidierte Übersicht über das gesamte Ökosystem zu bieten.

Die Microsoft Operations Management Suite erfüllt diese Anforderungen. Sie überwacht die Integrität kritischer Workloads wie Active Directory und SQL Server fortlaufend, stellt sicher, dass alle lokalen und Remotesysteme mit aktuellen Programmen und Signaturen vor Schadsoftware geschützt sind, analysiert Petabyte an Daten aus dem Rechenzentrum und der Cloud, um eine konsolidierte Ansicht von Trends zu erstellen und unterstützt virtuelle Maschinen unter Windows und Linux lokal, in Azure und in Amazon Web Services. Cloud-übergreifende Verwaltungslösungen von Accenture, RightScale und VMware (um nur einige zu nennen) bieten ähnliche Features an.

Kapitel 11

Neue Anwendungsmodelle



Der Umzug von Anwendungen in ein Infrastructure-as-a-Service (IaaS)-Modell in der Cloud ist im Grunde genommen einfach und bietet wie bereits besprochen zahlreiche Vorteile. Sowohl IT als auch Projektbeteiligte können jedoch enormen Nutzen aus der Transformation ziehen, indem sie die nativen Fähigkeiten der Cloud nutzen: neue Anwendungsmodelle und cloudeigene Dienste. In den nächsten Kapiteln besprechen wir, wie Unternehmen die einzigartigen Features der Cloud optimal zu ihrem Vorteil nutzen können. Wir beginnen in diesem Kapitel mit einer Besprechung der Eigenheiten und Vorteile neuer Anwendungsarchitekturen.

Cloud Computing hat die Art und Weise revolutioniert, wie wir Anwendungen entwickeln, testen und bereitstellen. Durch die leichte Verfügbarkeit von Cloud-Ressourcen können neue Anwendungen schneller bereitgestellt und aktualisiert werden. Aus diesem Grund entstanden neue Methoden zum Support dieser schnellen Modelle für die Entwicklung und Bereitstellung von Anwendungen.

Was bedeutet Transformation?

Wir hatten vor kurzem ein Gespräch mit einem Start-up-Unternehmen, das eine Internet of Things (IoT)-Anwendung entwickelt. In diesem Fall handelt es sich um die Erfassung der Ergebnisse eines medizinischen Heimgeräts über das Internet. Die Architektur der Anwendung ist relativ einfach (siehe Abbildung 11-1).

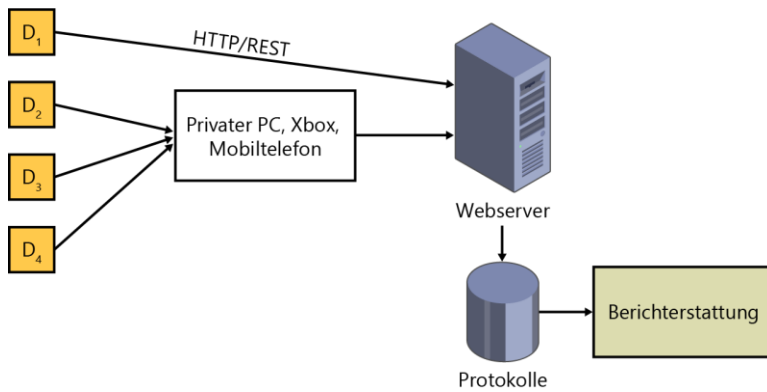


Abbildung 11-1: Einfache IoT-Architektur

Wie Sie sehen, sendeten die Geräte Daten über das REST-Protokoll entweder direkt an einen Webserver oder über einen Router an den Server. Der Server wiederum verarbeitete die Daten und speicherte sie in einer Datenbank, in der sie danach in einer intern entwickelten Berichtenanwendung angezeigt wurden.

Wir stellten ein paar einfache Fragen:

- Was passiert, wenn das Unternehmen ungemein erfolgreich wird und jederzeit zehntausende Geräte online unterstützen muss?
- Wie würde das Unternehmen die Elastizität unterstützen?
- Wie könnte präventive oder prädiktive Wartung durchgeführt werden?
- Wie könnte es die unzuverlässigsten Lieferanten für seine Geräte entlarven?
- Wie könnte das Unternehmen schnell neue Berichte hinzufügen?

Wir haben dem Unternehmen empfohlen, die Funktionen in die Cloud zu integrieren. In der vorgeschlagenen Architektur (siehe Abbildung 11-2) vernetzt das Start-up seine Geräte einfach mit den verschiedenen Diensten.

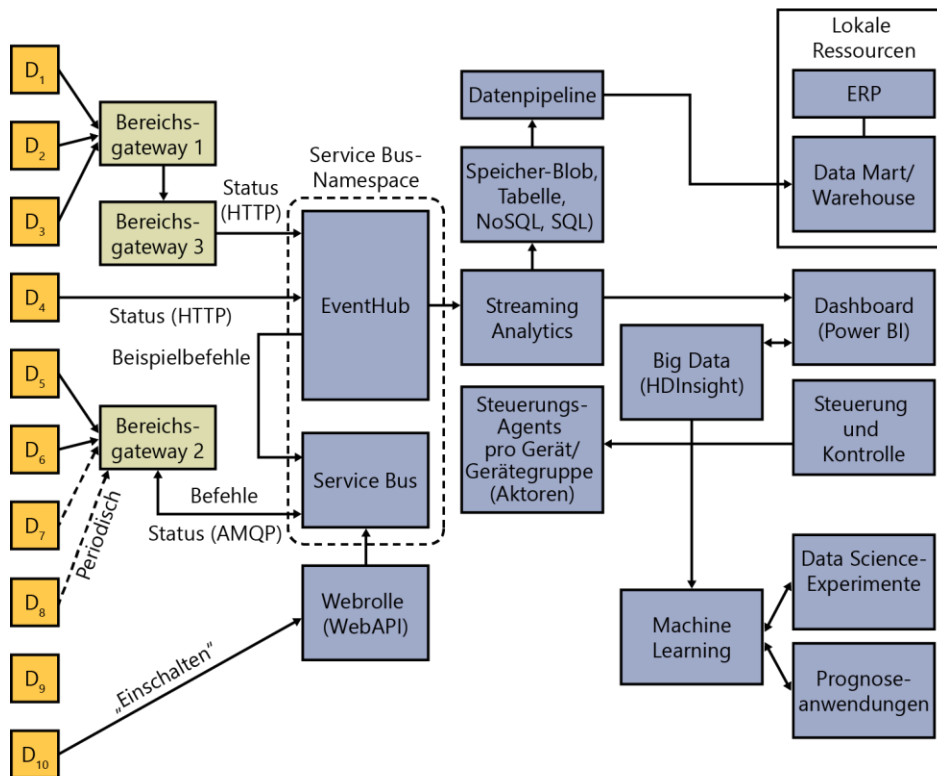


Abbildung 11-2: Umfassende End-to-End-IoT-Anwendung

Mit Microsoft Azure Event Hubs, das den gewaltigen Durchsatz bei der Ereignisaufnahme unterstützt, kann die Anwendung des Startups problemlos auf beliebig viele Geräte skaliert werden. Die erhaltenen Daten werden in Azure Tables gespeichert, wo automatisch zwei Replikate aufbewahrt werden. Dadurch wird gewährleistet, dass keine Daten verloren gehen. Die Daten können mit MapReduce-Programmen in Azure HDInsight in großem Umfang analysiert werden, und die Benutzer können in Echtzeit programmgesteuerte Befehle geben und die Abläufe kontrollieren. Machine Learning-Anwendungen können programmiert werden, um ansteigende Tendenzen im Absatz oder bei Defekten von Teilen vorherzusagen. Zudem können sämtliche Daten in einem intuitiven und optisch ansprechenden Dashboard visualisiert werden, jeweils mit *minimalem Programmieraufwand*.

Kurz gesagt: Eine früher ziemlich beschränkte Anwendung wurde sehr schnell zu einer innovativen, erkenntnisreichen und bahnbrechenden Anwendung.

Dabei geht es natürlich hauptsächlich darum, dass Anwendungen mit verschiedenen cloudeigenen Fähigkeiten auf zahllose Arten erweitert werden können. In den nächsten Abschnitten werden wir diese neuen Modelle ausführlich besprechen.

Platform-as-a-Service (PaaS)

Wie bereits besprochen ist IaaS der vermutlich einfachste Ansatz für den Umzug von Anwendungen in die Cloud. IaaS bietet zahlreiche Vorteile, wie etwa die Übergabe der Verantwortung für das Rechenzentrum an den Cloudanbieter. Für eine richtige *Transformation* zu einem cloudbasierten Modell besteht der nächste Schritt darin, Anwendungen speziell für die Cloud zu entwickeln.

IaaS hat aber auch gewissen Einschränkungen: Sie sind weiterhin für die Verwaltung der Systemsoftware, des Betriebssystems und der Datenbank für Ihre Anwendung zuständig, einschließlich regelmäßiger Patches und Softwareupgrades. IaaS ist also lediglich der *erste Schritt*, wenn Sie die Vorteile der Cloud voll ausschöpfen möchten.

Wie in Abbildung 11-3 gezeigt, müssen Sie in Platform-as-a-Service (PaaS)-Modellen lediglich *Ihre Anwendung* (in blau dargestellt) *pflegen*, während die Systemsoftware vom Cloudanbieter bereitgestellt und gewartet wird. Zusätzlich ermöglichen PaaS-Angebote in der Regel nahtlose Skalierbarkeit und Resilienz in Form von horizontaler Skalierung und Datenreplikation, und PaaS kann mit Cloud-Diensten wie Microsoft Azure Active Directory (Azure AD) für eine stabile Identitätsverwaltung kombiniert werden.

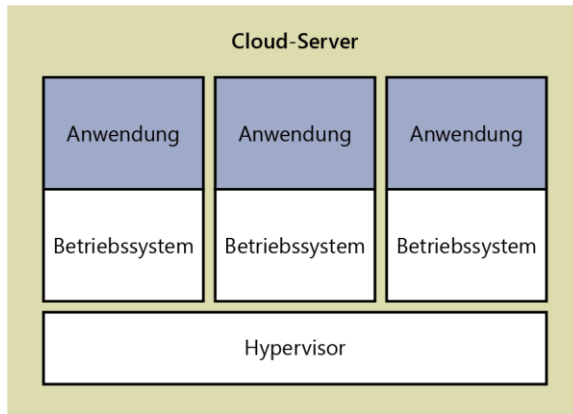


Abbildung 11-3: Platform as a Service

Azure App Service Web Apps sind ein Beispiel für eine Möglichkeit, um eine skalierbare Website in der Cloud mit geringem Aufwand bereitzustellen. Microsoft stellt die zugrunde liegende Webinfrastruktur (Betriebssystem, Netzwerkstapel, Speicher, Sprachunterstützung und Skalierbarkeitsfunktionen) bereit, die den Aufwand beim Verwalten einer groß angelegten Webanwendung verringert. Die Konfiguration der Skalierbarkeits-, Sicherheits- und Überwachungsfunktionen in einer Web Apps-Anwendung ist einfach. Web Apps verbinden sich auch mit allen anderen Diensten, die die Cloud für umfangreiche Anwendungen anbietet (mehr dazu später).

Azure Cloud Services sind das Cloud-Gegenstück zu den Drei-Schichten-Geschäftsanwendungen von vor zehn Jahren. In Cloud Services besteht eine Anwendung aus drei Komponenten: einer *Webrolle*, die im Prinzip ein Web-Front end ist, das unabhängig von den anderen Teilen der Anwendung skaliert werden kann, einer *Workerrolle*, die Berechnung und Verarbeitung im Hintergrund ermöglicht (vergleichbar mit der Geschäftslogik im Drei-Schichten-Modell), und *persistentem Speicher* mithilfe einer Azure-aktivierten Version von SQL Server (Azure SQL Database). Auch wenn eine gewisse Umgestaltung erforderlich ist, um eine vorhandene Anwendung zu Cloud Services zu verschieben, ist dies dennoch recht einfach, da das Modell absichtlich so ähnlich wie das Drei-Schichten-Modell gestaltet wurde.

Container und Orchestrierung

PaaS-Anwendungen haben einen Nachteil: Obwohl der Cloud-Anbieter die Betriebssystemumgebung bereitstellt und wartet, werden Betriebssystem und Anwendung weiterhin als virtuelle Maschine ausgeführt und haben daher dieselbe Startzeit wie ein vollwertiges Betriebssystem.

Einer der wichtigsten neuen Trends im Bereich der Anwendungsarchitektur ist das sogenannte *Containermodell*, das nach den allgegenwärtigen Frachtcontainern benannt wurde, die wir jeden Tag auf Schiffen und auf LKWs sehen. Wie diese physischen Container sind auch Softwarecontainer standardisierte Pakete, die mühelos übertragen und schnell bereitgestellt werden können.

Um das Containermodell zu verstehen, ist es sinnvoll, einen Vergleich zu IaaS und PaaS herzustellen. In beiden Fällen verwaltet ein *Hypervisor* mehrere Betriebssysteminstanzen auf einem Server (in IaaS wird das Betriebssystem von Ihnen bereitgestellt, in PaaS vom Cloud-Anbieter). Auf jedem Server werden also möglicherweise mehrere (sehr große) Betriebssysteme gleichzeitig und parallel ausgeführt, jeweils mit komplett duplizierten Funktionen (jedes BS hat einen Dateimanager, ein Netzwerksystem usw.).

Im Containermodell (Abbildung 11-4) *teilen sich* Anwendungen eine einzelne Instanz des Betriebssystems. Sowohl Microsoft Windows als auch die verschiedenen Linux-Distributionen wurden verbessert, um die benötigte Isolierung zu garantieren, sodass jede Anwendung das Betriebssystem scheinbar „besitzt“. Die Anwendungen werden für die Bereitstellung auf containerfähigen Systemen „verpackt“.

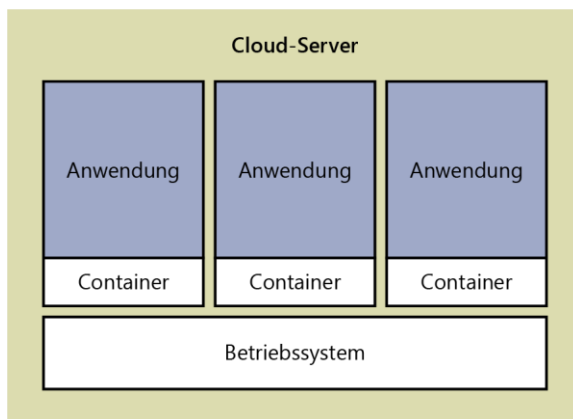


Abbildung 11-4: Containerarchitektur

Dieses Modell ermöglicht einen deutlich schnelleren Anwendungsstart, da der Mehraufwand für das Laden eines gesamten Betriebssystems für jede App entfällt. Außerdem können Sie standardisierte und mobile Pakete oder *Abbilder* erstellen, z. B. ein Abbild für einen Webserver oder eine Datenbank, und diese Abbilder ohne komplexe Installation bereitstellen.

Container ermöglichen zudem eine viel effizientere Nutzung der Hardware, da die Anzahl der tatsächlichen Betriebssysteminstanzen pro Server reduziert wird (unter Umständen auf nur eine Instanz).

In einer typischen Containerumgebung werden Instanzen von Containern auf einer Reihe von Servern ausgeführt, einem *Cluster*. Dazu zählen oft Webserver, Back-End-Logik, Suchfunktionen, Echtzeit analytics usw. Die Software, mit der die entsprechende Anzahl an Instanzen bereitgestellt und auf kontrollierte Art und Weise aktualisiert, Fehler verarbeitet und Skalierungsvorgänge durchgeführt werden, nennt man auch *Orchestrierungssoftware* (Abbildung 11-5). Die meisten Orchestrierungsdienste enthalten Tools, mit denen Administratoren Regeln erstellen können, z. B. um zu verhindern, dass sich zwei bestimmte Containertypen auf demselben Server befinden, oder um Failover und Wiederherstellung auf kontrollierte Art und Weise zu verarbeiten. Beispiele für bekannte Orchestrierungsprodukte sind Kubernetes, Mesosphere, Docker Swarm und Deis sowie Microsoft Service Fabric, das wir im weiteren Verlauf noch ausführlicher behandeln werden.

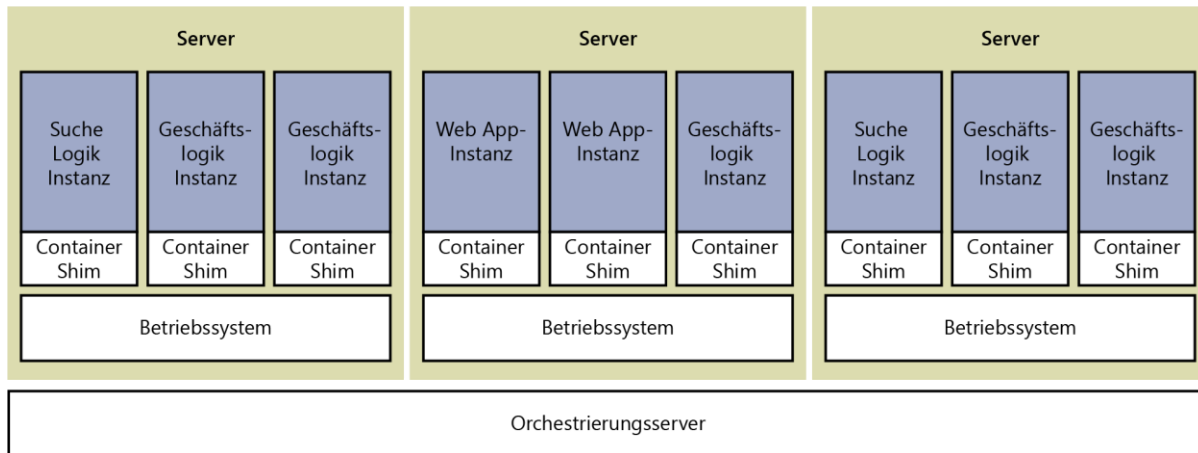


Abbildung 11-5: Orchestrierung

Container sind ein guter Weg, um Legacy-Anwendungen in die Cloud umzuziehen und die Effizienz zu steigern. Die interne IT-Abteilung von Microsoft hat zahlreiche Anwendungen in Docker-Container auf Azure verschoben und dabei vier wichtige Vorteile identifiziert:

- Effizientere Auslastung der Infrastruktur
- Standardisierte Infrastrukturkonfiguration
- Isolierte Anwendungsumgebungen
- Bessere Portabilität und Wiederverwendbarkeit der Anwendungen

Nach Abschluss dieser Machbarkeitsstudie mit 10 Anwendungen hatte die Microsoft-IT-Infrastruktur eine um 400 Prozent höhere Dichte als ohne Container, und die Gesamtinfrastruktur wurde um 300 Prozent reduziert.

Microservices

Der Begriff „Microservices“ wurde vor wenigen Jahren geprägt. Er beschreibt den Ansatz, dass große, monolithische Anwendungen in kleinere, komponentenbasierte Dienste zerlegt werden können. Im Beispiel in Abbildung 11-5 sehen Sie nur drei ziemlich grobkörnige Anwendungskomponenten: Webserver, Geschäftslogik und Datenbank.

Stellen Sie sich jedoch die Entwicklung einer E-Commerce-Anwendung vor. Möglicherweise könnten die Ressourcen besser genutzt werden, wenn ein Team die Katalogkomponente entwickelt, ein anderes Team die Bestellungskomponente und ein drittes Team eine kommerzielle oder Open-Source-Suchfunktion von einem externen Anbieter integriert. In diesem Fall können die Komponenten unabhängig voneinander entwickelt und aktualisiert werden.

Microservices sind eher ein architektonischer Grundsatz (oder Entwurfsmuster) als eine tatsächliche Technologie. Microservices können in IaaS, PaaS oder mit Containern entwickelt werden.

Azure Service Fabric bietet eine Plattform für die Entwicklung geschäftskritischer Anwendungen, die wiederum für die Entwicklung von Microservice-basierten Lösungen verwendet werden können. Service Fabric wurde vor der Einführung als allgemein verfügbares Produkt intern von Microsoft als Hostinglösung für die Azure-Kerninfrastruktur sowie für andere Microsoft-Dienste wie Skype for Business, Intune, Azure Event Hubs, Azure Data Factory, Azure Cosmos DB, Azure SQL Database, Dynamics 365 und Cortana getestet und ist daher extrem stabil.

Service Fabric hostet und orchestriert eine Vielzahl von Anwendungsmodellen, inklusive der Container- und Aktorenmodelle (siehe nächster Abschnitt), wurde für extreme Zuverlässigkeit und Verfügbarkeit entwickelt und bietet automatische Skalierung, parallele Upgrades und Selbstreparatur nach Fehlern.

Aktorenmodell

Das *Aktorenmodell* ist ein weiteres Tool für Cloud-Entwickler (siehe Abbildung 11-6). Ein „Aktor“ ist ein einfaches, normalerweise nicht besonders großes Objekt in der Cloud mit einer eindeutigen Identität, das mit anderen Aktoren kommunizieren kann und seinen Status beibehält. Aktoren bilden normalerweise physische Objekte wie Personen oder Geräte ab. Für diese Technologie wurde neuerdings auch der Begriff *digitaler Zwilling* geprägt: Das Aktor-Objekt ist eine digitale Spiegelung von Objekten in der echten Welt. Das *Aktor-Framework* abstrahiert Infrastrukturkonzepte wie Server, d. h. Aktoren können miteinander kommunizieren, ohne wissen zu müssen, ob sie sich auf unterschiedlichen physischen Servern befinden.

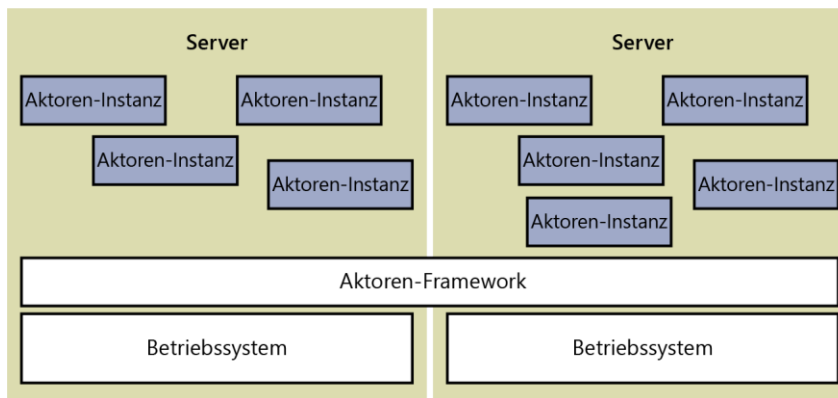


Abbildung 11-6: Modellarchitektur für Aktoren

Ein mögliches Nutzungsbeispiel ist ein Onlinespiel, in dem jede Aktoren-Instanz einen Spieler abbildet und dessen Status wie die aktuelle Punktzahl, den Aufenthaltsort im Spiel und eine Liste der anderen teilnehmenden Spieler enthält.

Hinweis Eine der weltweit größten Spieleserien, Microsoft Halo von 343 Studios, verwendet das Aktorenmodell auf genau diese Art und Weise.

Sie können Aktoren auch verwenden, um eine große Anzahl an IoT-Geräten zu verwalten. Dies ist besonders effizient, wenn es sich um viele gleiche Geräte handelt, z. B. überwachte Sensoren. Jede Aktoren-Instanz kann Statusupdates von einem bestimmten Sensor erhalten, z. B. einem Drucksensor, und anschließend automatisch einen Aktor benachrichtigen, der ein Ventil oder ein anderes Gerät für die entsprechende Maßnahme steuert.

Resilienz in der Cloud

Machen Sie sich bewusst, dass die Kosten in der Cloud durch den Einsatz von Standardhardware niedrig gehalten werden. In der Vergangenheit haben Unternehmen bei der Skalierung oft High-End-Geräte gekauft. In der Cloud wird die Kapazität stattdessen durch *horizontale* Skalierung erweitert. Anstatt einen riesigen Supercomputer zu kaufen, setzen Sie also viele verteilte Computer ein, und müssen sich entsprechend auf gelegentliche Ausfälle vorbereiten.

Resilienz bedeutet die Fortsetzung der Funktionen nach Ausfällen, beispielsweise wenn ein Server defekt ist, indem mehrere Instanzen einer Anwendung oder eines Diensts bereitgestellt werden, oder nach einem katastrophalen Ausfall, beispielsweise mit Azure Site Recovery, wie in Kapitel 10 besprochen.

Verwenden Sie das folgende Modell für die Planung der Resilienz Ihrer Anwendung:¹³

1. **Definieren** Sie Ihre Verfügbarkeitsanforderungen anhand Ihrer Geschäftsanforderungen.
2. **Entwickeln** Sie die Anwendung im Hinblick auf Resilienz. Gestalten Sie Ihre Architektur anhand bewährter Praktiken, und identifizieren Sie anschließend mögliche Schwachstellen in dieser Architektur.
3. **Implementieren** Sie Strategien zur Erkennung von Ausfällen und für die Wiederherstellung.
4. **Testen Sie** die Umsetzung durch die Simulation von Fehlern und das Auslösen erzwungener Failover.
5. **Stellen Sie** die Anwendung in der Produktion bereit, indem Sie einen zuverlässigen, wiederholbaren Prozess verwenden.
6. **Überwachen Sie** die Anwendung zur Erkennung von Fehlern. Durch Überwachung des Systems können den Zustand der Anwendung messen und nötigenfalls auf Vorfälle reagieren.
7. **Reagieren Sie** auf Vorfälle, die manuelle Eingriffe erfordern.

Das Maß, in dem Sie Resilienzfeatures implementieren sollten, hängt teilweise von Ihren Geschäftsanforderungen ab. Beraten Sie sich mit Ihren Geschäftspartnern über die gewünschten Recovery Time Objective (RTO) und Recovery Point Objective (RPO), die wir auch im Kapitel 10 besprechen. Beachten Sie auch Nutzungsmuster, z. B. wann die Anwendung oder das System unbedingt verfügbar sein müssen. In solchen Fällen empfiehlt sich auch in weniger kritischen Zeiten die Hinzunahme von zusätzlichen Cloud-Ressourcen.

Ein Blick auf Ihr gewünschtes Service Level Agreement (SLA). Tabelle 11-1 zeigt die potenzielle kumulative Ausfallzeit für unterschiedliche SLA-Ebenen.

Tabelle 11-1: Service-Level Agreements

SLA	Ausfallzeit pro Woche	Ausfallzeit pro Monat	Ausfallzeit pro Jahr
99 %	1,68 Stunden	7,2 Stunden	3,65 Tage
99,9 %	10,1 Minuten	43,2 Minuten	8,76 Stunden
99,95 %	5 Minuten	21,6 Minuten	4,38 Stunden
99,99 %	1,01 Minuten	4,32 Minuten	52,56 Minuten
99,999 %	6 Sekunden	25,9 Sekunden	5,26 Minuten

Ob Engineering-Bemühungen für mehr „9“ ihr Geld wert sind, kommt auf das Geschäftsszenario an.

Ein weiterer wichtiger Aspekt sind die kumulativen SLAs. Ein System wie das in Abbildung 11-7 verwendet eine Webanwendung und eine SQL-Datenbank. Anstehende Updates werden einer Azure-Warteschlange hinzugefügt, wenn die Datenbank nicht verfügbar ist.

¹³ <https://docs.microsoft.com/azure/architecture/resiliency/>

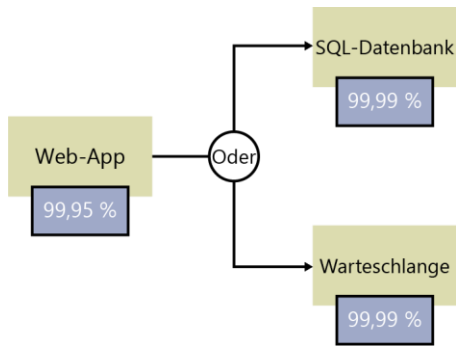


Abbildung 11-7: System mit Komponenten verschiedener SLAs

Jede von ihnen hat ein jeweiliges SLA. Eine einfache Rechnung zeigt das kumulative SLA aller Teile:

$$\text{Datenbank oder Queue} = 1,0 - (0,0001 \times 0,001) = 99,99999 \%$$

$$\text{Webanwendung und (Datenbank oder Queue)} = 99,95 \% \times 99,99999 \% = \sim \mathbf{99,95 \%}$$

„Serverlose“ Anwendungen

Mit sogenannten „serverlosen Anwendungen“ hat das äußerst aufregende und neue Anwendungsmodell einen sehr irreführenden Namen (es gibt natürlich einen Server. Sie müssen ihn aber weder erstellen, verwalten oder dafür bezahlen). In vielerlei Hinsicht haben serverlose Anwendungen eine sehr attraktive Amortisierung, weil dafür keine Programmierung erforderlich ist.

Serverlose Anwendungen sind Anwendungen, die aus bestehenden Komponenten zusammengesetzt werden können, ohne dass dafür eine Programmierung erforderlich ist. So können Sie Anwendungen schnell und kostengünstig entwickeln.

Hier ist ein einfaches Beispiel. Nehmen wir an, dass Sie als Leiter des Kundenservice wissen möchten, wenn Kunden eine Fehlfunktion Ihres Produkts melden. Mit Microsoft Flow können Sie Twitter auf Erwähnungen des Hashtags #BrokenAcmeWidget hin überwachen; bei einer Erwähnung kopiert Flow sie automatisch in Ihren lokalen Slack-Kanal (ein beliebtes Tool für Zusammenarbeit), wie die Abbildung 11-8 zeigt.

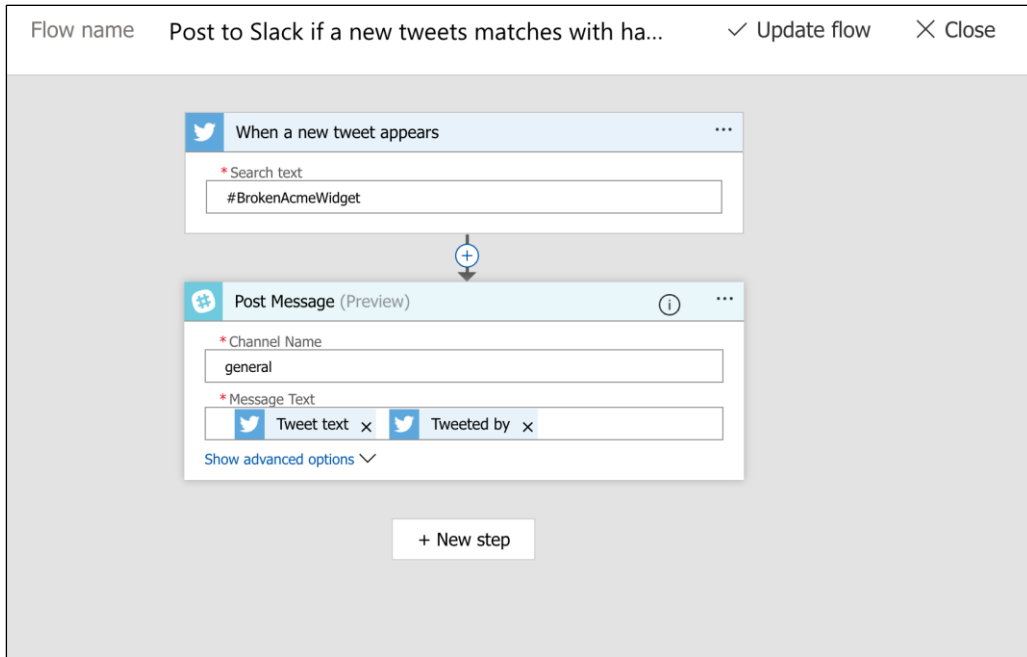
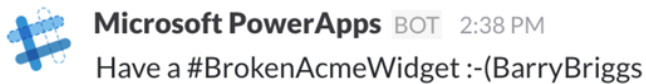


Abbildung 11-8: Die serverlose Cloudanwendung Microsoft Flow

Das würden Sie in Slack sehen:



Jetzt möchten Sie als Kundendienstmitarbeiter vielleicht einen Problemfall eröffnen, ein Formular ausfüllen und den Prozess in Gang setzen, der eine Antwort auf die Meldung Ihres unzufriedenen Kunden bietet. Eine formularbasierte Anwendung zu erstellen erforderte normalerweise Ressourcen in der Entwicklung. Aber dank den neuen serverlosen Funktionen (hier die Anwendung PowerApps von Microsoft) gehört das der Vergangenheit an. Hier wird das Formular entwickelt und bereitgestellt. Bei Verwendung setzt es einen weiteren Flow in Bewegung, wie Abbildung 11-9 zeigt.

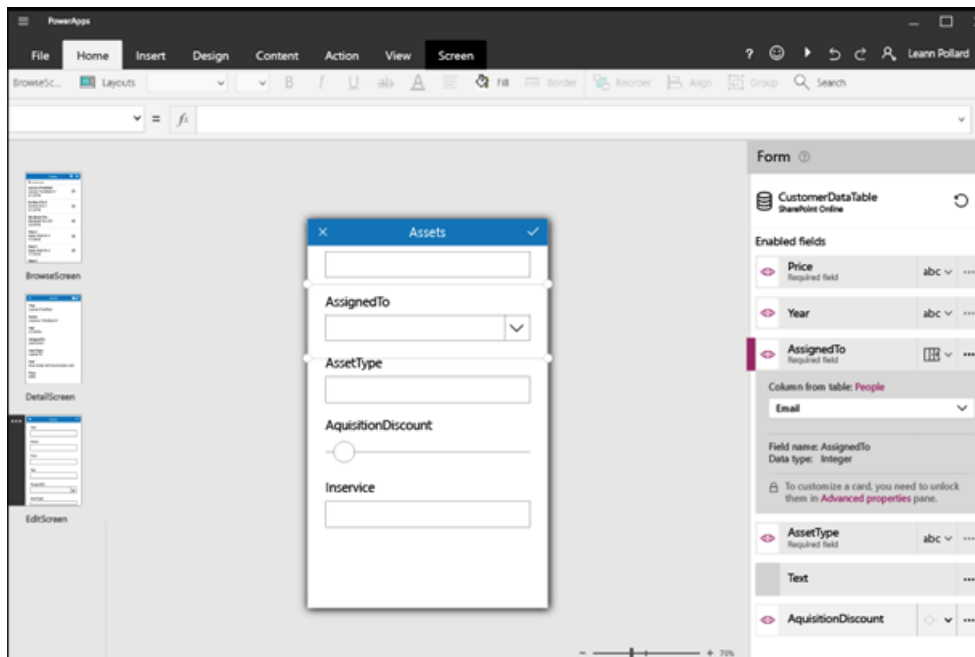


Abbildung 11-9: Demo zu Microsoft PowerApps

Und es könnte schließlich Fälle geben, in denen eine benutzerdefinierte Verarbeitung für ein bestimmtes externes Ereignis, wie etwa einen Tweet, sinnvoll sein würde. Ihre Entwickler können hierbei serverlose „Funktionen“ entwickeln, die andere wiederum nutzen können, ohne den Tweet durch einen Code anbinden zu müssen, wie beispielsweise ein Modul zur Stimmungsanalyse. Die Entwicklung ist in diesem Fall so gestrafft, dass eine interaktive Entwicklungsumgebung (IDE) wie Microsoft Visual Studio nicht notwendig ist. Die Programmierung findet direkt im Azure-Portal statt, wie Abbildung 11-10 zeigt.

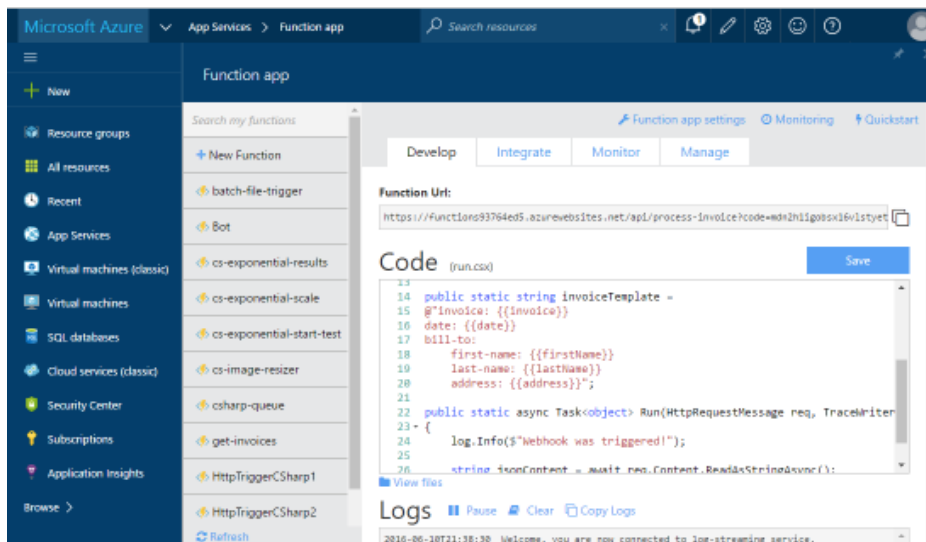


Abbildung 11-10: Azure Functions

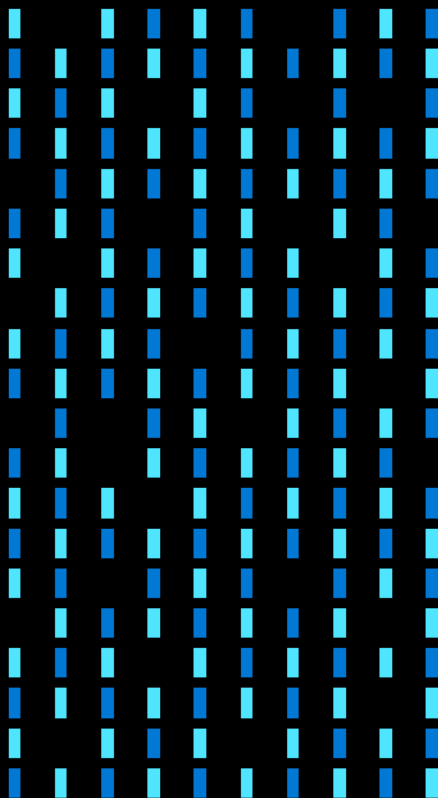
Auch hier können Sie die Funktionen nach der Erstellung in einer beliebigen Anzahl von Anwendungen wiederverwenden, indem Sie sie einfach zusammenziehen.

Diese serverlosen Funktionen könnten sogar ein neues Zeitalter von Cloud-Anwendungen einläuten. Cloud-Anwendungen entwickeln sich immer mehr zu einem Lego-Block-Modell von „serverlosem“ Computing. Darin erstellen und zahlen Sie nur für Ihre Geschäftslogik, in der Bruchstücke von Datenverarbeitungslogik zusammengesteckt werden, um eine vollständige Geschäftsanwendung zu erschaffen.

Infrastruktur? Natürlich gibt es eine (wie schon gesagt ist „serverlos“ nicht wörtlich zu nehmen), aber sie ist nicht auf den ersten Blick zu erkennen. Der Cloud-Anbieter verwaltet, konfiguriert und aktualisiert die Server und stellt darüber hinaus ihre Verfügbarkeit sicher. Sie können sich dabei ganz auf Ihre Geschäftslogik konzentrieren. Und dabei haben Sie nicht einen einzigen Server bereitgestellt. Ihr Code beruht einzig und allein auf der Geschäftslogik und nicht auf Administrationsskripts oder Code ohne Wert für Ihr Unternehmen. Ihre Entwickler konzentrieren sich auf das Wachstum Ihres Unternehmens. Am wichtigsten dabei ist, dass sie eine umfangreiche und intelligente End-to-End-Anwendung erstellt haben, und dazu haben Sie nur bereits bestehende Blöcke von Logiken aneinandergereiht.

Kapitel 12

Alles dreht sich um
die Daten



Bisher haben wir uns verstärkt auf die „Rechen“-Seite der Cloud konzentriert. Die Cloud bietet aber auch sehr kostengünstig großzügige Speicherkapazität. Daten wie Telemetrie oder Benutzerkommentare, die wir einst vernachlässigt haben, können wir somit jetzt erfassen, verwalten und analysieren. In den letzten paar Jahren ist eine Vielzahl von Datenbanktechnologien zu Tage getreten, um all diese verschiedenen Datentypen bewältigen zu können. In diesem Kapitel untersuchen wir, wie traditionelle Datenbank Technologien auf die Cloud, die neuen „-NoSQL“ Datenverwaltungstechnologien, umgestiegen sind. Außerdem beleuchten wir, wie Sie differenzierte Analyse funktionen nutzen können, um neue Erkenntnisse aus all diesen Daten ziehen zu können.

Es ist heutzutage selbstverständlich, dass Informationen als Vermögenswert eingestuft werden, und zwar so sehr, dass schon die Einbeziehung in die Bilanzen erwogen wurde. Informationen sind der Grundstein jeder gefällten Entscheidung, jedes Investments und praktisch jeder offiziell getätigten Handlung eines Unternehmens. Von IT-Managern wird verlangt, die Entscheidungsträger mit aktuellen und präzisen Informationen und außerdem mit detaillierten Analysen der Informationen zu versorgen, um neue Insights aus den Kunden zu gewinnen. In den meisten Fällen hüten IT-Manager also nicht nur Geschäftsgeheimnisse, sondern auch die persönlichen Informationen zu Mitarbeitern, Partnern und Kunden. Die Datenverwaltung ist also jetzt das Herzstück des modernen Unternehmens – und der Cloud?

Zwischen Rohdaten und Informationen zu unterscheiden, ist nicht unüblich. Wir könnten sagen, dass die Technologie uns die Tools zur Verfügung stellt, um die Daten in Informationen zu verarbeiten. Diese riesige Menge an Daten aber heutzutage zu sammeln und zu speichern, führt Unternehmen an ihre Grenzen, was sie dadurch lösen möchten, die Verwaltung dieser Datenmenge an Cloud-Speicherressourcen auszulagern. Die Cloud bietet glücklicherweise viele Optionen zur Speicherung, Verwaltung und Analyse von Daten und zur Verwertung dieser großen Datenmengen.

Enterprise Data Management vor der Cloud

Vor dem Aufkommen der Cloud haben Unternehmen ihre Daten vornehmlich auf zwei Arten organisiert und verwaltet. Wir wollen uns beide ansehen.

Strukturierte Datenverwaltung

Das Herzstück der Informationsverwaltung von Unternehmen war vor nicht allzu langer Zeit noch eine relationale Datenbank mit sorgfältig definierten Tabellen, in deren Zeilen und Spalten sich hochgradig „strukturierte“ Daten befanden. Relationale Datenbankverwaltungssysteme (RDBMS) hatten einen enormen Wert für Unternehmen und haben ihn immer noch. Ihr vielleicht größter Nutzen liegt in der inhärenten *Integrität*, dass die Informationen in der Datenbank auf jeden Fall als zuverlässig angesehen werden konnten. Wenn Sie beispielsweise Geld von Ihrem Girokonto auf Ihr Sparkonto überweisen wollten und währenddessen der Server abgestürzt ist, wurde Ihnen das Geld ersetzt. Wir sprechen also bei RDBMS-Transaktionen von „ACID“, was für atomar, konsistent, isoliert und dauerhaft steht.

Wie die Abbildung 12-1 zeigt, hat sich im Laufe der Zeit eine Art Hierarchie unter den RDBMS-Anwendungen herauskristallisiert. Anwendungen *verweisen* auf Master-Datenverwaltungsanwendungen, deren Daten sich ziemlich selten ändern, die jedoch wichtige Informationen (z. B. Kundenname und -adresse oder die Bestandteile eines Produkts) beinhalten; Master- (oder Referenz-)Datensysteme soll für die Verteilung und Synchronisierung dieser Daten über mehrere Anwendungen sorgen. So sollen z. B. Kundendaten von Customer Relationship Management [CRM], Enterprise Resource Planning [ERP] und Supportsystemen geteilt werden.¹⁴

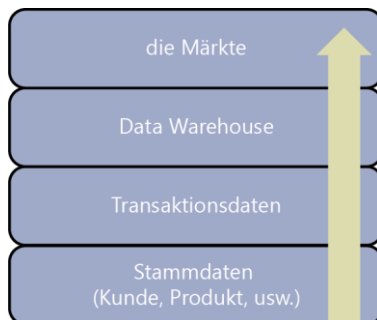


Abbildung 12-1: Enterprise Data Management in den 1990er-Jahren

Im Gegensatz dazu werden Transaktionssysteme regelmäßig aktualisiert. In ihnen spielen sich die meisten und wichtigsten Unternehmensvorgänge ab, wie Kundeneinkäufe, Finanztransaktionen, Lieferkettenverwaltung usw. In einem großen Unternehmen gibt es viele Transaktionssysteme, die verschiedene Teile oder Bereiche eines Unternehmens widerspiegeln. Transaktionssysteme sind auf schnelle und interaktive Antworten ausgelegt.

Transaktionsdaten würden für Berichte regelmäßig zu Rechenzentren übertragen werden, die große Mengen an historischen Daten verwalten. Die Daten werden dann aus dem Rechenzentrum an Data Marts gesendet. Das sind Datenbank-Anwendungen, die eine bestimmte Funktion erfüllen, wie z. B. Predictive Analytics oder Kampagnenverwaltung.

¹⁴ Uns ist bewusst, dass dies vielleicht eine (übermäßige) Vereinfachung der Theorien von den Data Warehouse-Experten Bill Inmon und Ralph Kimball ist. Insbesondere Inmon vermutet, dass Marts in das Warehouse aggregieren, im Gegensatz zu dem von uns angezeigten Beispiel. Beides ist gültig: Unsere Sicht weist einfach darauf hin, dass es eine Zeit lang eine relativ direkte Taxonomie von Datenverwaltungstools gab.

Wie die Abbildung 12-1 zeigt, fließen die Daten in diesem Modell immer aufwärts. Es ist nur selten der Fall, dass Änderungen in den unteren Systemen vorgenommen werden, beispielsweise die Aktualisierung einer Kundenadresse im Master-Datensystem.

Im Rahmen des Supports dieser Datenbanken hat sich ein engagiertes Team von Datenbank-Administratoren (DBAs) um Backups und Wiederherstellungen, um die Änderungen des Layouts (wie z. B. neue Spalten) oder den fehlerfreien Transfer von Daten von einer Datenbank in die andere gekümmert.

Unstrukturierte Daten

Es gibt neben strukturierten Daten natürlich noch viele andere Arten von Daten. Menschen nehmen für gewöhnlich Informationen wie dieses Buch in einem *unstrukturierten* Format auf. Texte, Audio- und Videodateien oder Bilder sind Beispiele für unstrukturierte Daten. Der Zuwachs der Menge dieser unstrukturierten Daten ist durch das immense Wachstum des Internets zu erklären. Viele dieser Daten erfordern bestimmte Fähigkeiten, wie z. B. Videos zu streamen, um Benutzer zu unterstützen, die den Spielkopf bewegen, um Thumbnails zur Verfügung zu stellen, und so weiter.

Anwendungen in der Cloud erzeugen darüber hinaus mit Daten wie der Telemetrie sehr große Datenmengen.

Enterprise Data Management im Zeitalter der Cloud

Datenverwaltung in der Cloud birgt demzufolge viele Vorteile und Möglichkeiten. Bei Rechenleistung ist es so, dass Sie nur für die Speicherressourcen zahlen, die Sie auch tatsächlich nutzen.

Durch das Design der Cloud entstehen jedoch noch weitere Vorteile. Die Ausfallsicherheit bei Cloud-Speichern ist im Gegensatz zu teuren Storage Area Networks (SANs) dadurch gegeben, dass sie zwei voneinander unabhängige Kopien erstellt, die gegen Aufpreis auf verschiedene geographische Orte verteilt sind. Ein solches Konstrukt wird *Geo-Redundanz* genannt.

Andere Vorteile hängen von dem jeweiligen Dienst ab, worauf wir in den nächsten Abschnitten eingehen werden.

Wichtige Speicherkonzepte

Die grundlegendsten Speicherabstraktionen in der Cloud sind das *Blob*, die *Datei*, die *Tabelle* und die *Warteschlange*. Wir wollen uns nun jeden Bestandteil ansehen.

Blobs

Der Begriff „Blob“ ist eine Abkürzung für *Binary Large Object*. Dieser Begriff ist etwas irreführend, da ein Blob weder groß noch binär sein muss. Ein Blob besteht lediglich aus einem unstrukturierten „Haufen von Bits“. Das kann von einem Bild über eine Textdatei bis zu einem Video alles sein, was digital gespeichert werden kann. Blobs sind so etwas wie individuelle Dateien, obwohl es eine gesonderte „Datei“-Abstraktion gibt, auf die wir gleich zu sprechen kommen.

Blobs werden häufig für Webassets wie Bilder verwendet.

In Microsoft Azure es gibt mehrere Arten von Blobs, wobei die maximale Größe eines einzelnen Blobs etwa 4,75 TB beträgt.

Dateien

Viele Anwendungen können mit Dateien umgehen und verwenden dabei insbesondere das weit verbreitete Server Message Block (SMB)-Protokoll, um auf Dateien in Netzwerken zuzugreifen. Die „Datei“-Abstraktion unterstützt dabei die Kompatibilität.

Tabellen

In Azure bestehen Tabellen aus einfachen Schlüssel-Wert-Paaren, die Anwendungen ein Grundmaß an strukturierten Daten bieten. Aktuell beträgt die maximale Größe einer Tabelle in Azure 500 TB.

Warteschlangen

Wie der Name schon sagt, sind Warteschlangen eine skalierbare Möglichkeit zum Senden von Daten zwischen verschiedenen Anwendungskomponenten. Warteschlangen regeln Aktivitätsschübe in Anwendungen und sorgen dafür, dass Anwendungen oder Server währenddessen diese Schübe bewältigen können.

Relationale Daten in der Cloud

Der Bedarf an leistungsstarken Konsistenz- und Abfragefunktionen relationaler Datenbanken ist natürlich in Zeiten der Cloud nicht weniger geworden, sondern eher stetig gewachsen.

Die Nutzung relationaler Datenbanken in der Cloud bietet jedoch bestimmte Vorteile. Neben Microsoft haben viele Datenbankanbieter ihre Datenbankprodukte in Plattform-as-a-Service (PaaS)-Angebote umgewandelt. Hierbei sind die Anbieter der Plattform für die Aktualisierungen der Systemsoftware und andere Wartungsarbeiten verantwortlich. Die Kunden solcher als „Database as a Service“ bezeichneten Angebote zahlen, wie bei allen Cloud-spezifischen Angeboten, nur für die tatsächlich genutzte Kapazität.

Als besonderes Feature gibt die Azure SQL Database von Microsoft Empfehlungen an seine Benutzer, wie sie die Leistung ihrer Datenbanken steigern können. So könnten Indizes erstellt oder gelöscht werden oder Probleme bei Schemata behoben werden.

Im Azure SQL Data Warehouse bietet Microsoft auf Petabyte-Ebene die oben beschriebene Funktionalität und kombiniert sie mit den Vorzügen der Cloud. Wie das verwandte Azure SQL wird das Azure SQL Data Warehouse vollständig verwaltet und kann nach Bedarf angepasst werden.

Hinweis Bei „verwalteten Diensten“ können Sie SQL Server und viele weitere Produkte in einer virtuellen Maschine (VM) als Infrastructure as a Service (IaaS) betreiben. In diesem IaaS-Modell müssen Sie das Betriebssystem und auch die Datenbanksoftware warten. Bei einem verwalteten Dienst wie der Azure SQL Database übernimmt jedoch der Cloud-Anbieter – in diesem Fall Microsoft – die gesamte Wartung der Systemsoftware. Eine solche verwaltete Variante eines Softwareprodukts ist in der Regel sehr viel kostenintensiver als ein IaaS-Modell.

Die zunehmende Bedeutung von NoSQL-Datenbanken

Die ein oder andere neue Architektur zur Speicherung und Verwaltung von Daten ist in den letzten Jahren zu Tage getreten, die relationale Datenbanken zwar nicht ersetzt, aber ergänzt. Notwendigerweise erstrecken sich solche Datenbanken oft über viele Server, weil die gesammelte Datenmenge sehr schnell anwächst.

Eine davon ist die „Dokument-Datenbank“, in der Texte für gewöhnlich in Form von JavaScript Object Notation (JSON) gespeichert werden. Ein sehr einfaches „Dokument“ im JSON-Format sehen Sie hier:

```
{
  "Vorname" : "Max",
  "Nachname" : "Mustermann",
  "Tags" : ["Sportbegeistert", "Autor", "Programmierer"],
  "Beruf" : "Softwareentwickler"
}
```

Datenbanken für Dokumente ersetzen jedoch nicht relationale Datenbanken, bieten aber in bestimmten Situationen viele Vorteile. Dokument-Datenbanken sind weitaus nicht so starr und aufwendig ausgelegt wie relationale Datenbanken. Dokumente müssen sich nicht an ein festgelegtes Schriftbild halten. Sie können bei Bedarf neue Felder (Spalten) hinzufügen, wobei solche Änderungen an relationalen Datenbanken recht mühsam sind. Unterschiedliche Implementierungen von Dokument-Datenbanken bieten verschiedene Stufen an ACID-Transaktionen.

Zur starken Einschränkung einer Konsistenz (wie etwa bei ACID-Transaktionen) können Sie zwar Dokument-Datenbanken wie CosmosDB von Azure (ehemals DocumentDB), MongoDB von Mongolabs oder die Open-Source CouchDB konfigurieren. Sie können aber auch auf eine *letztendliche Konsistenz* ausgerichtet werden, was bedeutet, dass andere verwandte Aufzeichnungen mit der Zeit miteinander konsistent werden. Dabei wird ihre Entnahme *letztendlich* als Anzahlung erscheinen).

Eine Dokument-Datenbank dürfte für eine Banking-Anwendung wenig sinnvoll sein. Sie eignet sich jedoch hervorragend für die Nachverfolgung von Beiträgen aus sozialen Netzwerken, wie z. B. die Tweets eines Benutzers, die Zeit und das Thema, wobei eine Liste für jedes Element angelegt wird. Ein Produktkatalog könnte eine weitere sinnvolle Anwendung sein.

Eine andere Form der NoSQL-Datenbank ist die Graph-Datenbank, in der Daten nicht in Reihen und Spalten, sondern als Referenzen untereinander gespeichert werden. Eine Graph-Datenbank kann beispielsweise eine Personenbeschreibung speichern. Diese Aufzeichnung verweist dann auf weitere „Freunde“ oder auf Datensätze von Lieblingsfilmen, Essen oder Kommentaren in sozialen Netzwerken.

Die Entwicklung einer Graph-Datenbank in einem relationalen Modell ist durchaus möglich. Sollte die Anzahl fremder Schlüssel aber zu groß sein, ist eine Graph-Datenbank wie Neo4j sinnvoller. Jede Datenbank unterstützt andere Warteschlangen-Sprachen, wobei manche benutzerdefiniert, manche SQL-basiert sind. Andere wie GraphDB verlassen sich bei ihrer Architektur auf das Resource Description Framework des World Wide Web Consortium (RDF).

Letzten Endes läuft die Diskussion darauf hinaus, dass im letzten Jahrzehnt unzählige hocheffiziente Datenverwaltungsoptionen aus dem Boden geschossen sind. Denken Sie deswegen darüber nach, welche neuen Quellen und Anwendungen für Ihre Daten in Betracht kommen.

Big Data und Bigger Data

Wir können aber über die benutzerdefinierten Datenbanken hinaus die riesigen Datenmengen sammeln, die mittlerweile anfallen. Die Statistiken dürften bekannt sein: Jeder Mensch erstellt jede Sekunde 1,7 Megabyte. Bis 2020 werden wir etwa 44 *Zettabyte* Daten (44 Billionen Gigabyte) erstellt haben. Oder an bestimmten Tagen nutzen eine Milliarde Menschen das soziale Netzwerk Facebook.

Die Quelle all dieser Daten ist eindeutig: Hochgeladene Fotos und Videos, Server-Protokolldateien, Softwaretelemetrie, soziale Medien, Hardwaretelemetrie, Daten zur Nachverfolgung von Handys, Webbrowsering oder viele andere menschliche Aktivitäten.

Tatsächlich lagern viele Regierungen diese riesigen Datenmengen in die Cloud aus (die Vereinigten Staaten beispielsweise unter <http://www.data.gov>, das Vereinigte Königreich unter <http://www.data.gov.uk>, Frankreich unter <http://data.gouv.fr> usw.). Andere Unternehmen machen Daten gegen eine Gebühr über das Internet verfügbar. Solche Daten können lokale Masterdatenquellen beispielsweise erweitern oder gar ersetzen oder zusätzliche Marketingerkenntnisse bereitstellen. Die Nutzung dieser Daten kann Ihrem Modell zusätzliche Insights verschaffen.

Nicht nur die schiere Menge oder die Geschwindigkeit, in der diese Big Data auftreten, sondern auch die vielen verschiedenen Datentypen stellen eine Herausforderung dar. Viele verweisen deswegen auf die „drei Vs“ der Big Data: Volume, Velocity und Variety (Volumen, Geschwindigkeit und Vielfalt).¹⁵

In all diesen Daten steckt bekanntlich auch eine Menge *Informationen*. Durch die sorgfältige Analyse von Server-Protokolldateien lässt sich beispielsweise erkennen, dass hin und wieder ein misslungener Anmeldeversuch aus einem fremden Land verzeichnet ist, was möglicherweise auf einen Cyberangriff hindeutet. Durch die Analyse von Kommentaren auf Twitter können Sie auch erkennen, wie Leute beispielsweise zu Ihrem Produkt stehen. Das wird als „Stimmungsanalyse“ bezeichnet.

Die Speicherung und Analyse sogenannter „Big Data“ gehört mittlerweile zum Tagesgeschäft in Unternehmen. Für gewöhnlich verwenden Big Data-Architekturen das Open-Source-Projekt Hadoop, das nach dem Stoffelefanten des Sohnes der Erfinders benannt wurde. Es werden auch Nachfolgeprojekte von Hadoop genutzt. Sein Kernalgorithmus MapReduce ist auf die Abfrage und Analyse sehr großer Datensätze ausgelegt.

Um Ihnen ein sehr einfaches Beispiel von MapReduce in Aktion nahezubringen, schieben Sie für einen Moment Ihren gesunden Menschenverstand beiseite. Stellen Sie sich vor, sie wollten jedes Vorkommen des Ausdrucks „Abraham Lincoln“ im Internet finden. Dazu gibt es mehrere Möglichkeiten, aber Sie könnten zunächst alle Webseiten, die mit einem „A“ beginnen, auf eine gigantische (hier müssen Sie wie angekündigt Ihren gesunden Menschenverstand beiseite lassen) Festplatte in einem Computer speichern, dann alle Seiten, die mit einem „B“ beginnen, auf eine Festplatte in einem anderen Computer, und so weiter. Danach zählt jeder Computer, wie oft „Abraham Lincoln“ auf der jeweiligen Festplatte vorkommt. Schließlich sendet jeder Computer seine Ergebnisse an einen Zentralcomputer, der alle Zwischenergebnisse addiert und die endgültige Anzahl angibt.

Wir haben also ein kleines Kommando, oder Programm, an die alphabetisierten Computer gesendet und den Code den Daten zugeordnet. Das ist eines der Kernkonzepte der Big Data. Wir aktualisieren also nichts oder führen Transaktionen aus, sondern prüfen nur, welche Insights gewonnen werden könnten.

Eine ganze Serie von Softwareprodukten und Technologien, wie z. B. Hive (SQL-ähnliche Anfragen), Pig (Sprache zur Codierung von MapReduce-Programmen) und viele andere haben Hadoop ihre Existenz zu verdanken. Spark ist dabei von besonderem Interesse, weil es durch In-Memory-Transaktionen bessere Leistungen bringt. Als HDInsight werden neben Hadoop und Spark auch HortonWorks und Cloudera (für Hadoop) sowie Databricks (für Spark) in Azure mit jeweiligen Zusatzfunktionen unterstützt. Das Open-Source-Projekt Cassandra von DataStax bietet eine Big Data-Lösung mit sehr guter Leistung und SQL-ähnlichen Abfragefunktionen.

¹⁵ Das Konzept wurde von Gartner-Analyst Doug Laney im Jahr 2001 eingeführt.

Der Data Lake

Ein „Data Lake“ ist eine Methode, riesige Mengen von Daten in vielen verschiedenen Formaten zu speichern. Das von Hadoop verwendete Dateisystem ist dabei eine Variante von Data Lakes. Data Lakes werden oft mit Data Warehouses verglichen, wobei es jedoch einen gravierenden Unterschied gibt: Data Warehouses sind eine Art Sammelstelle für *strukturierte* (relationale) Daten, und normalerweise müssen die Daten aus transaktionalen Systemen umgewandelt werden, um in die Modelle (Schemata) der Warehouses zu passen.

Data Lakes speichern im Gegensatz dazu Rohdaten, ganz egal, in welchem Format und wie strukturiert oder unstrukturiert sie sie erhalten.

Analyse-Dienste und Datenvisualisierung

Business Intelligence (BI)-Anwendungen erfordern oftmals spezielle Datenbanken, mit denen Sie den Daten auf den Grund gehen und sie auf verschiedene Arten sammeln können. Außerdem muss die Datenbank die Ausführung von Algorithmen, wie z. B. die Segmentierung oder Regression verschiedener Daten beherrschen. In der relationalen Welt treiben sogenannte *Cubes*, also multidimensionale Datenstrukturen, diese Analytics-Dienste an. Daten aus vielen unterschiedlichen Quellen werden oft in Cubes zusammengeführt.

Azure Analytics Services bieten diese Funktionen, die an SQL Server Analytics Services von Microsoft erinnern, als Cloud-Dienst in Azure an. Sie funktionieren genau wie andere Cloud-Dienste nach dem Prinzip „Pay as you go“. Dabei müssen Sie für Azure Analytics Services nur dann zahlen, wenn Sie sie auch tatsächlich in Anspruch nehmen, beispielsweise am Ende eines Quartals.

Wie die Abbildung 12-2 zeigt, sind Azure Analytics Services eng in das Visualisierungstool von Microsoft Power BI integriert und bietet somit nicht nur bei Analytic Services, sondern auch bei unzähligen Datendienstleistern einfache, aber leistungsstarke „Drill-Down“-Visualisierungen der Informationen.

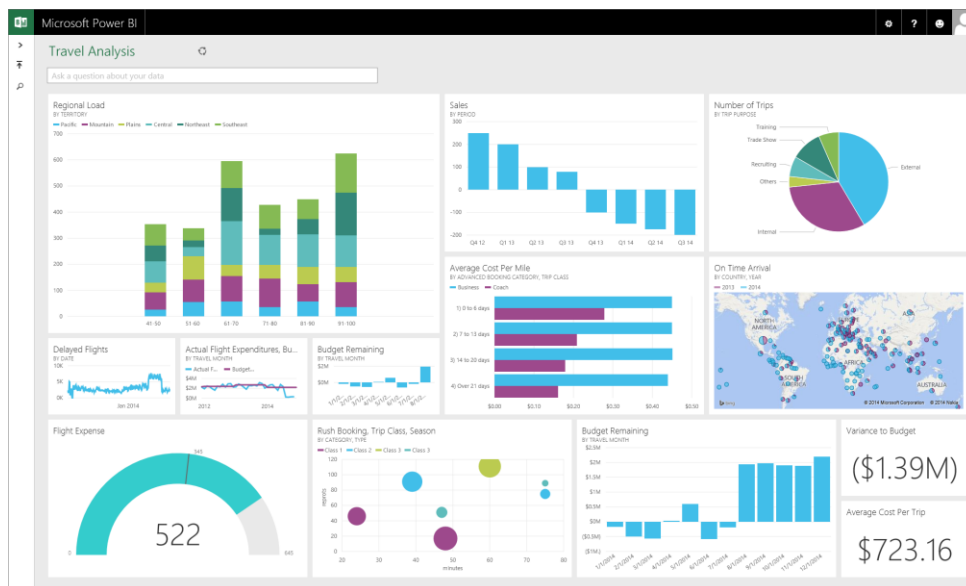
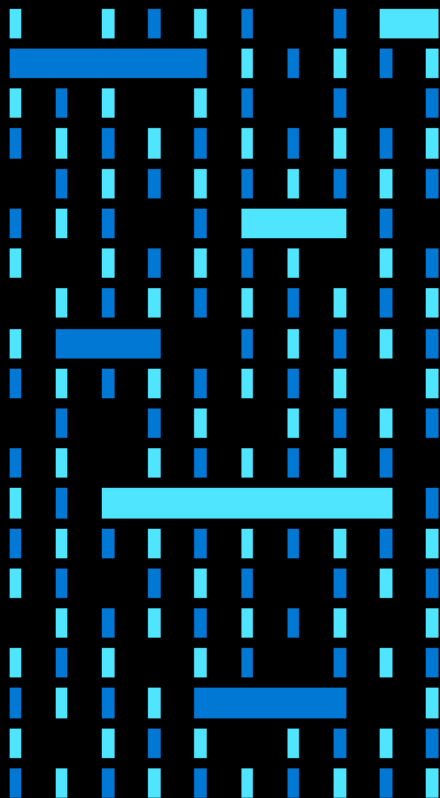


Abbildung 12-2: Power BI-Visualisierung

Kapitel 13

Entwickeln Sie mit KI Ihr
Unternehmen erfolgreich weiter



Das Feld der Künstlichen Intelligenz (KI) fristete jahrelang in akademischen Rechenlabors und anderen Forschungseinrichtungen ein Schattendasein. Aber die beträchtliche Rechenleistung und der fast unendliche Speicherplatz der Cloud haben der KI den Weg in den Mainstream geebnet und das Computing revolutioniert. Mit Ihrem Computer zu sprechen, also seine Spracherkennungsfunktion zu nutzen, war einst mit Fehlern behaftet. Das gehört jedoch nun der Vergangenheit an und ist nun weitestgehend fehlerfrei. Die KI-Technologie ermöglicht es nun zudem mehr und mehr, „in die Zukunft zu sehen“, also vorherzusagen, wann ein Teil womöglich nachgibt oder wann ein Patient wahrscheinlich wiederaufgenommen wird.

Spätestens seit HAL aus 2001: Odyssee im Weltraum war das Prinzip des „intelligenten Computers“ sowohl ein Gegenstand der Science Fiction als auch der Forschung. In den 1960er-Jahren schrieb der MIT-Professor Joseph Weizenbaum ein kurzes Programm – gerade einmal ein paar hundert Zeilen lang –, das die Methodik eines Psychotherapeuten simulierte. Das Programm hieß „Eliza“ und fragte Benutzer danach, was sie beschäftigte. Danach gab es die Antworten als Frage zurück, wie z. B. „Mein Hund hasst mich.“ „Warum hasst Ihr Hund Sie?“ und so weiter.

Seitdem hat sich in der modernen künstlichen Intelligenz einiges getan. Im folgenden Kapitel geben wir deshalb eine kurze Übersicht darüber, warum sie im Zeitalter der Cloud ihren zweiten Frühling erlebt. Außerdem sprechen wir über die Art der Technologie dahinter. Danach diskutieren wir einige der Probleme und Möglichkeiten, für die KI nützlich sein kann.

Was umfasst KI und Machine Learning?

Im Großen und Ganzen bezeichnet KI menschenähnliche Fähigkeiten in Computern aus: Sicht und Sprache, Erkennung und Schlussfolgerungen, Mustererkennung und Vorhersagen. Einige Ansätze sind in den letzten Jahrzehnten gekommen und auch wieder gegangen, wobei sich einige bei besser werdender Technologie einer gewissen Beliebtheit erfreuen konnten, während andere verworfen wurden.

Drei wichtige Erkenntnisse zeichnen für das derzeitige Interesse am Wiederaufleben der KI verantwortlich:

- Für die Arbeit mit künstlicher Intelligenz brauchen Sie riesige Mengen an Speicherplatz
- Sie benötigen ebenfalls enorme Mengen an Verarbeitungskapazität
- Sowohl die großen Mengen an Speicherplatz als auch die Verarbeitungsmöglichkeiten sind in der Cloud verfügbar

Viele Menschen setzen die Begriffe „künstliche Intelligenz“ mit „Machine Learning“ gleich. Für eine präzise Terminologie verwenden wir den Begriff *Machine Learning* als Unterbegriff des größeren Bereichs der künstlichen Intelligenz, in der wir Modelle mit großen Mengen an historischen Daten antrainieren, die wir dann nutzen, um neue Daten auszuwerten. Im folgenden konzentrieren wir uns auf die Machine Learning-Disziplin innerhalb der künstlichen Intelligenz.

Machine Learning: Grundlagen

Die Konzepte „künstliche Intelligenz“ und „Machine Learning“ hören sich zwar etwas mysteriös an, sie sind jedoch relativ einfach. Hier ist eine kurze Einführung in die Kunst und Wissenschaft von Machine Learning.

Nehmen wir an, Sie wünschen sich ein Programm, das vorhersagen kann, wann ein bestimmtes Teil einer Maschine ausfällt. Sie haben Terabytes und Terabytes an Log-Dateien, und Sie haben eine Liste der Teile, die versagt haben. Jeder Datensatz der Log-Datei identifiziert das Teil, die eindeutige ID, den Lieferant, wann es hergestellt wurde, wann es gekauft wurde, wann und von wem es zuletzt gewartet wurde, die Computer-ID, in der das Teil installiert ist, sowie 50 andere Datenelemente.

Ihre Aufgabe ist es – angesichts der ID des Teils – zu bestimmen, wann es ausfallen wird.

Ein Machine-Learning-Anwendung hat vielleicht die Antwort darauf. Der erste Schritt besteht in der *Aufteilung* Ihrer historischen Daten. Die Idee ist, dass Sie ein Modell mit einem Teil der Daten *antrainieren* und dann herausfinden, ob das Modell die Ergebnisse im anderen Teil der Daten korrekt vorhersagt.

Der nächste Schritt – das Antrainieren – ist die verarbeitungsintensivste Phase beim Machine Learning. Dabei werden große Mengen an Daten aufgenommen und mathematische Korrelationen zwischen den Variablen entwickelt. Eine Vielzahl dieser mathematischen Algorithmen existiert bereits und ist allgemein verfügbar. Es ist oft nützlich, die Lernphase mit mehreren Algorithmen durchzuführen und herauszufinden, welches davon die besseren Ergebnisse liefert.

Im letzten Schritt nehmen Sie das trainierte Modell und geben rohe, nicht „antrainierte“ Daten ein, um zu sehen, ob es die Ergebnisse exakt prognostiziert, d. h. welche Teile in den nicht antrainierten Daten (Log-Datei) ausgefallen sind. Dies wird „Scoring“ genannt. In unserem Beispiel der Fehlerprognose wird jede Teile-ID der nicht trainierten Daten in Betracht gezogen und eine Ausfallwahrscheinlichkeit zurückgegeben. Diese wird anschließend mit der tatsächlichen Ausfallrate verglichen. Wenn die Ergebnisse zufriedenstellend sind – z. B. höher als 95 Prozent – können Sie das trainierte Modell in der realen Welt einsetzen.

Sie können dann die Log-Dateien in einer neuen Anwendung in Ihr trainiertes Modells eingeben und eine Warnung anzeigen, wenn ein Teil sich dem Ausfall nähert. Daraufhin können Sie proaktiv einen Servicemitarbeiter entsenden, um das Teil zu ersetzen und so die Kundenzufriedenheit zu verbessern und Ihre eigenen Kosten zu senken.

Dies ist im Kern der Wert von Machine Learning, wenn auch nur minimal erklärt.

Abbildung 13-1 zeigt, wie die Entwicklung dieses Modells im Microsoft Azure Machine Learning Studio aussieht. Beachten Sie, dass es sich hier nur um einen einfachen grafischen Workflow handelt – in diesem Fall ist der verwendete Algorithmus eine lineare Regression.

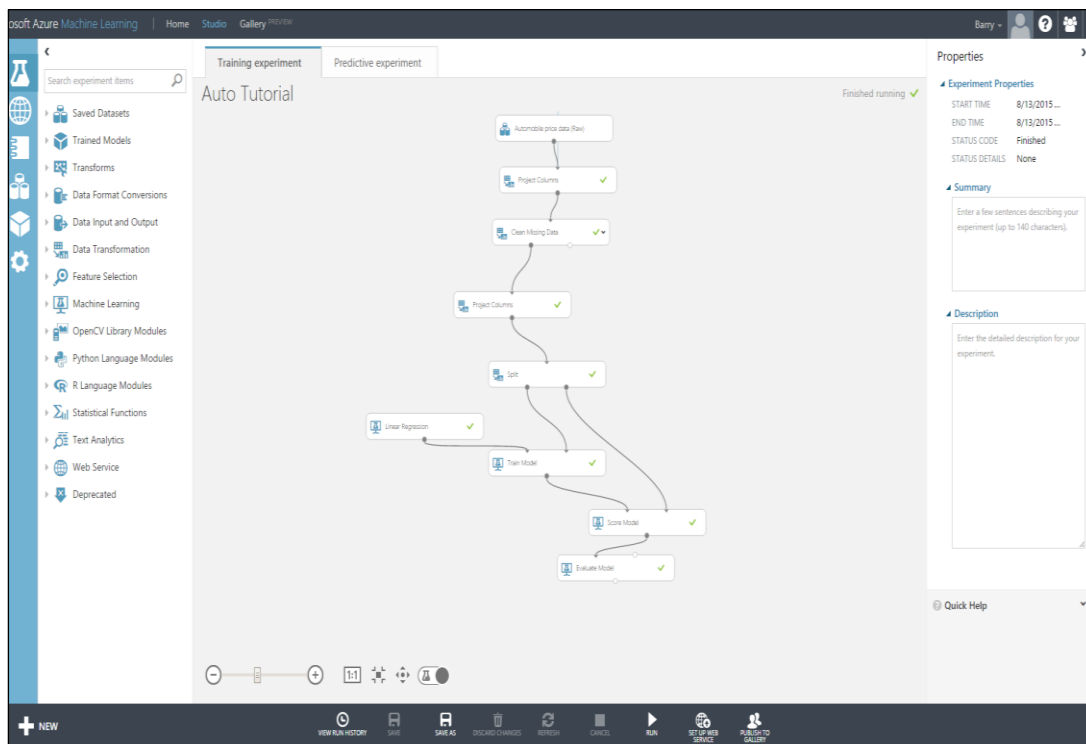


Abbildung 13-1: Azure Machine Learning

An dieser Stelle lohnt es sich, eine Weisheit zu bestätigen, die jeder Datenforscher kennt. Der schwierigste Teil bei der Entwicklung eines Algorithmus für Machine Learning (wie in Abbildung 13-1 gezeigt) ist die Garantie, dass die Daten „sauber“ sind, d. h. dass es sich bei allen Terabytes um zulässige Werte und keine verbotenen Daten usw. handelt. (Dieses Problem ist jedem bekannt, der je einen umfangreichen Prozess für die Extraktion, die Transformation und das Laden von Daten [ETL] entworfen hat.) Im Modell in der Abbildung gibt es einen Schritt, der „Fehlende Daten löschen“ heißt – eine der vielen integrierten Funktionen für die Datenbereinigung.

Überwachtes Lernen im Vergleich zu unüberwachtem Lernen

Machine Learning unterscheidet zwischen sogenanntem *überwachtem* Lernen und *unüberwachtem* Lernen. In unserem Beispiel wussten wir, welche Teile ausfielen, also haben wir unser Modell im Erkennen von Kombinationen und Zusammenhängen von Variablen ausgebildet, so dass es einen Ausfall akkurat vorhersagen kann. Der Score-Wert unseres Modells basierte auf unseren bereits vorhandenen Kenntnissen und wir haben es mit einer größeren Datenmenge neu trainiert oder einige Parameter geändert oder einen anderen Algorithmus ausgesucht, wenn die Ergebnisse nicht zu unserer Zufriedenheit ausfielen. Dies ist ein Beispiel von überwachtem Lernen.

Im unüberwachten Lernen haben wir kein bestimmtes Ziel vor Augen, wie z. B. die Wahrscheinlichkeit eines ausfallenden Teils zu bestimmen. Vielmehr sind wir auf der Suche nach Mustern in den Daten. Es gibt zwei Hauptprobleme, die durch unüberwachtes Lernen gelöst werden. Das erste ist *Clustering*. Hierbei handelt es sich um das Entdecken von Gruppen in großen Datasets, die Sie vorher nicht kannten wie z. B. Kunden, die nach Kaufverhalten gruppiert sind. Das zweite ist das Entdecken von *Assoziationen* oder bisher unbekannten Zusammenhängen zwischen Datenelementen in großen

Datenmengen. So finden Sie zum Beispiel heraus, dass Kunden, die ein bestimmtes Produkt kaufen auch dazu neigen, ein anderes verwandtes Produkt zu kaufen.

Neuronale Netze

Bei neuronalen Netzen handelt es sich um einen weiteren mathematischen Algorithmus, den wir bei Machine Learning nutzen können. Wie der Name sagt, ahmt ein neuronales Netz die Tätigkeit der Zellen im Gehirn nach. Im Wesentlichen handelt es sich hierbei um die Idee, dass eine kleine Reihe Code einen Teil der Daten analysiert und eine Wahrscheinlichkeit erstellt, dass eine bestimmte Bedingung erfüllt ist. Diese „Neuronen“ fließen dann in andere Neuronen über und analysieren größere Daten-„Brocken“, die letztlich bestimmen, ob eine bestimmte Bedingung erkannt wurde. Neuronale Netze werden umfassend in sensorisch gesteuerten Anwendungen genutzt, wie bei der Spracherkennung und bei maschinellern Sehen.

Der Begriff *Deep Learning* wird für neuronale Netze mit vielen Ebenen angewendet.

Machine Learning mithilfe von Hardware beschleunigen

Wie vorhin schon erwähnt, ist der verarbeitungsintensivste Teil beim Machine Learning die Trainingsphase. Viele der Trainingsalgorithmen profitieren von einer *Parallelität*. Dabei werden viele Prozessoren gleichzeitig ausgeführt, die sich auf die verschiedenen Datenelemente auswirken.

Je mehr Prozessoren desto besser. Wie sich herausstellt, unterstützen leistungsstarke Grafikprozessoren (GPUs) in der Regel Hunderte oder Tausende von miteinander verbundenen Prozessoren. Die GPU-Beschleunigung kann Machine Learning um ein Vielfaches beschleunigen – manchmal sogar noch viel mehr. Neuronale Netze lassen sich beim Training und während des laufenden Betriebs gut in Grafikkarten aufnehmen (Inferenzen), da ein Software-„Neuron“ in einen einzigen Prozessor in der Grafikkarte geladen werden kann.

Grafikkarten haben jedoch einen Nachteil: sie sind in der Regel teuer und verbrauchen eine Menge Strom. Außerdem wurden Grafikkarten ursprünglich nicht speziell für Machine-Learning-Anwendungen sondern für Grafiken konzipiert (obwohl einige Anbieter die grafische Schaltung entfernt haben).

Zwei neue Ansätze bieten speziell für Machine Learning konzipierte Hardware an. Mehrere Cloud-Anbieter, darunter auch Microsoft, haben die Verfügbarkeit von benutzerdefinierten Field Programmable Logic Arrays (FPGAs) in ihren Cloud-Rechenzentren angekündigt. Sie können FPGAs (programmierbare integrierte Schaltungen) auf verschiedenste Weise konfigurieren, um Machine-Learning-Anwendungen auszuführen. Genau wie Grafikkarten verfügen sie über die parallele Verarbeitung bei wesentlich höherer Geschwindigkeit.

Eine ganz neue Technologie bettet neuronale Netze in Silikon ein und erstellt Chips aus Silikon-Neuronen. Diese *neuromorphen* Chips stecken noch in den Kinderschuhen (und sind noch nicht allgemein verfügbar), sie sind allerdings sehr vielversprechend.

Die Nutzung von künstlicher Intelligenz und Machine Learning

Wie wir bereits in diesem Kapitel erörtert haben, glauben wir, dass künstliche Intelligenz und Machine-Learning-Technologien die Geschäftsmodelle revolutionieren werden. In diesem Abschnitt untermauern wir diesen Punkt mit einigen Beispielen.

Bots und dialogorientierte Computer

Machine Learning bietet Anwendungen die Möglichkeit, natürliche Dialoge zu verstehen, d. h. die Art und Weise, wie wir durch Sprache miteinander kommunizieren. Das wiederum bietet uns die Möglichkeit einer „menschlicheren“ Interaktion mit Computern. Anwendungen, die mit Menschen durch Sprache kommunizieren, werden *Bots* genannt. Sie ermöglichen neue Formen der Kundenbeziehung und Intimität.

Dank der Verbindung von Bots mit unternehmensinternen Datenquellen finden Unternehmen immer mehr Wege, diese zu nutzen. Beispielsweise kann der Benutzer bei großen Websites mit Tausenden von Seiten den Bot ganz einfach fragen, wo er die benötigten Informationen findet („Wie melde ich ein Kind in der Schule an?“ oder „Wo bezahle ich meine Rechnung?“). So kann er die oft veraltete Navigation umgehen, die viele moderne Websites auszeichnet.

Prädikative Analysen

In unserem einfachen Beispiel über Machine Learning haben wir große Mengen an Log-Dateien verwendet, um den Ausfall von Teilen vorherzusagen. Der Wert dieser Art Vorkenntnisse ist für Unternehmen ganz enorm: durch das Verhindern unerwarteter Ausfallzeiten können Unternehmen auf Hochtouren arbeiten und so die Kundenzufriedenheit verbessern.

Einige Unternehmen haben sogar prädikative Analytics verwendet, um ihr Geschäftsmodelle vollkommen zu verändern. Anstelle von Investitionsgütern verkaufen sie etwas, was als „Geräte-als-Service“ bezeichnet werden könnte. Das heißt, sie erheben mithilfe von Telemetrie und prädiktiven Analytics eine Abo-Gebühr für die Betriebszeit des Geräts und vermeiden so Ausfälle.

Der britische Hersteller Rolls-Royce analysiert beispielsweise mithilfe der Cortana Intelligence Suite Telemetriedaten von Microsoft von Düsentriebwerken, die er verkauft. Durch eine frühzeitige Analyse von Anomalien kann so sichergestellt werden, dass die Motoren immer auf dem höchsten Leistungsniveau funktionieren – und dass die Flüge pünktlich sind.

Autonomie

Moderne Automobile werden mit einer Vielzahl von Sensoren ausgestattet, einschließlich LIDAR und Videosensoren. Im Laufe der Zeit soll das Fahren dadurch völlig autonom werden, wobei das Auto selbst eine situationsbezogene Aufmerksamkeit über die Straße, die Straßenbedingungen, den Verkehr und so weiter erhält. Das autonome Auto – genau wie Projekte in puncto Autonomie für LKWs, Boote, Drohnen usw. – stützt seine Entscheidungen auf Machine Learning. Maschinelles Sehen kann Objekte wie Fahrspurmarkierungen, Geschwindigkeitsbeschränkungsschilder und andere Autos auf der Straße erkennen. Mittels anderer Sensoren innerhalb des Autos kann sichergestellt werden, dass der Fahrer wach und aufmerksam bleibt, auch wenn das Auto alles unter Kontrolle hat. Das Auto erhält ständig Verkehrsmeldungen, sodass es im Voraus intelligent einen anderen Weg finden kann, wenn ein Stau erkannt wird.

Betrugsermittlung und andere Finanzanwendungen

Finanzdienstleistungen haben viel Verwendung für künstliche Intelligenz und Machine Learning. Dies ist angesichts des Umfangs der von finanziellen Transaktionen generierten Daten nicht anders zu erwarten. Betrugsermittlungsprogramme verwenden Machine Learning-Techniken, um beispielsweise die Unmengen von Daten auf der Suche nach ungewöhnlichen Mustern zu verarbeiten. Andere auf Machine Learning basierte Programme können Details von Finanzberichten analysieren (wie 10-K-Berichte) und diese mit früheren Zeiträumen oder Berichten der Konkurrenz vergleichen und so Anlageempfehlungen generieren.

Eine der interessantesten Verwendung der künstlichen Intelligenz in der Finanzbranche ist der wachsende Bereich der „Roboter-Berater“. Hierbei handelt es sich um durch künstliche Intelligenz gesteuerte Finanzberater, die ein Benutzer-Portfolio prüfen und Algorithmen anwenden, um Vorschläge zu unterbreiten. Roboter-Berater werden nur zu einem Bruchteil der Kosten eines menschlichen Beraters betrieben und helfen bei der Verwaltung von Pensionskassen wie einem 401(k)-Rentenplan und individuellen Rentenkonten sowie steuerpflichtigen Anlagekonten. Sie bieten ebenfalls eine automatisierte Beratung zur Altersvorsorge und andere Investitionen an.

Die Nutzung im Gesundheitswesen

Im Gesundheitswesen wird die künstliche Intelligenz in vielen Bereichen genutzt. Machine-Learning-Anwendungen können für eine maßgeschneiderte Behandlung große Mengen an Krankengeschichten von Patienten schnell scannen. Durch die Analyse einer einheitlichen Patientenakte und durch den Vergleich mit vielen anderen Datensätzen (mit entsprechendem gesetzlich vorgeschriebenen Datenschutz) können individuelle Behandlungspläne für schwere Erkrankungen wie Krebs erstellt werden. Pharmaunternehmen nutzen Machine Learning-Algorithmen, um schnell neue Medikamente zu entwickeln und die oft mühsamen und zeitaufwändigen alten Ansätze von Versuch und Irrtum zu vermeiden (eine Firma namens Atomwise nutzte beispielsweise künstliche Intelligenz, um zwei Medikamente zu entwickeln, die ein großes Potenzial für die Behandlung des Ebola-Virus haben).

Zusammenfassung

Wir hoffen, dass wir bewiesen haben, dass die in der Cloud ausgeführten Anwendungen von künstlicher Intelligenz das Potenzial haben, alle Aspekte von Enterprise-Computing zu revolutionieren. Auch wenn es verfrüht ist, hat künstliche Intelligenz Unternehmen bereits verwandelt oder ist dabei, diese weltweit zu verändern.

Zusammenfassung



Zusammenfassung

Wir haben die erste Ausgabe von *Enterprise Cloud Strategy* mit der Aussage abgeschlossen: „Die Auswirkungen von Cloud Computing auf Unternehmen und das Geschäft im Allgemeinen können nicht zu hoch eingeschätzt werden.“ Wir sind sicher, dass die zwei Jahre, die zwischen der ersten Ausgabe und dieser vergangen sind, das bewiesen haben!

Was haben wir also gelernt?

In Kapitel 1 haben wir die sogenannte Makroökonomie der Cloud angesprochen und gezeigt, wie Cloud-Anbieter Skaleneffekte erzielen können, mit der kein einziges Unternehmen mithalten kann. Wir haben ebenfalls einige der vielen Kosteneinsparungsmöglichkeiten sowie die geringeren Gesamtbetriebskosten in der Cloud und die Möglichkeiten zur Realisierung messbarer ROIs mithilfe von PaaS-Diensten beschrieben.

Wir begannen unsere Cloud-Reise mit der Definitionen von Schlüsselbegriffen – IaaS, SaaS, PaaS und Container, in Kapitel 2, und haben die Vor- und Nachteile dieser Begriffe diskutiert. Ein zentrales Thema des Buchs, das zuerst in Kapitel 2 und danach erwähnt wird, ist, dass diese unterschiedlichen Ansätze zur Cloud-Migration deutlich unterschiedliche Chancen bieten: wenn Sie eine On-Premises-Anwendung durch einen SaaS-Service ersetzen können, haben Sie die Kosten enorm reduziert. IaaS-Anwendungen beseitigen die Last der Infrastrukturverwaltung von Servern und Netzwerken. Das PaaS-Modell geht noch einen Schritt weiter als die Cloud-Anbieter und ist ebenfalls für das Betriebssystem, die Datenbank und die Wartung verschiedener Systemsoftware verantwortlich.

Wir haben den Weg in drei Phasen beschrieben: Experimentieren, Migration und Transformation, und vorsichtig darauf hingewiesen, dass Sie diese Phasen parallel ausführen können – und sollten – und sie nicht als aufeinander folgende Schritte betrachten.

In der Phase des Experimentierens verschieben Ihre Teams vielleicht ein paar risikoarme Anwendungen in die Cloud, was darauf abzielt zu lernen, wie Sie für die Cloud planen, den Cloud-Betrieb verwalten und Funktionen nutzen können, die nur in der Cloud verfügbar sind. Wir empfehlen Best Practices, wodurch das Experiment nicht auf eine einfache Migration begrenzt wird, sondern Sie die Gelegenheit nutzen und selbst so viele Cloud-Features wie möglich ausprobieren.

Wie bereits erwähnt wurde, ist die komplizierteste Phase die Migration, wobei der Großteil der IT-Infrastrukturanwendung in die Cloud verlagert wird. In Kapitel 5 haben wir einige Beispiele und Best Practices angesprochen und wie Sie die Cloud-Migration organisieren und verwalten. Dies beginnt mit der Erstellung eines Cloud-Strategieteam, das für das Festlegen von Prioritäten und das Verwalten der Migration verantwortlich ist. Sie sollten von Zeit zu Zeit auf die Abschnitte über die betrieblichen Auswirkungen zurückgreifen, da fast jede Funktion der Unternehmens-IT – von der Personalabteilung über das Finanzwesen und die Entwicklung bis hin zu den Abläufen – auf irgendeine Weise von der Cloud-Migration betroffen ist.

In Kapitel 6 haben wir den Prozess der Priorisierung Ihrer Anwendungen beschrieben und wie wichtig das Festlegen von Kriterien ist, durch die Priorisierungsentscheidungen getroffen werden. Wir haben einige Beispiele zur Durchführung aufgeführt, die auf unserer langjährigen Erfahrung basieren. Dann haben wir beschrieben, wie Sie Ihren Plan durchführen und einige der verfügbaren Tools vorgestellt, die Ihnen bei der Migration helfen. Wir haben einige der Best Practices angesprochen, mit denen Sie mithilfe einer durchdachten Cloud-Abonnementverwaltung finanzielle Transparenz erreichen können.

Wenn Sie Ihre Anwendungen in die Cloud verschieben und Ihr Unternehmen immer schnellere Versionen benötigt, können Sie die Nutzung der DevOps-Tools und der Methoden erweitern, die

Lean-Manufacturing-Techniken auf Ihre Software anwenden. Mit Tools wie Microsoft Azure Application Insights und Azure Monitor können Sie die Ressourcen überwachen, die Ihre Anwendung von einem Moment zum anderen verwendet, um zu garantieren, dass Sie die besten Kostenvorteile erzielen.

In Kapitel 9 haben wir zwei der wichtigsten Bereiche der Cloud erläutert: Governance und Sicherheit, für die wir ebenfalls eine Reihe von Empfehlungen und Best Practices anbieten. Hinsichtlich der Einhaltung gesetzlicher Vorschriften, ist es wichtig zu verstehen, über welche Zertifizierungen Ihr Cloud-Anbieter verfügt und wie die Verantwortung der Zuständigkeiten zwischen Ihren Anwendungen und Daten auf der einen Seite und der Cloud-Plattform, dem Rechenzentrum und der Infrastruktur-Software auf der anderen Seite aufgeteilt ist.

In Bezug auf die Sicherheit haben wir viele Tools und Methoden erstellt, um sicherzustellen, dass Ihre Anwendungen und Daten in der Cloud sicher sind. Sie sollten diese unbedingt verwenden und regelmäßig im Azure Trust Center überprüfen, dass Sie auf dem neusten Stand sind, da häufig neue Bedrohungen auftauchen.

In Teil III, *Transformation*, sprachen wir über die Nutzung der Cloud und der verfügbaren Dienste in der Cloud, um nicht nur Kosten zu senken und Ihre Effizienz zu steigern, sondern die Funktionen Ihrer Anwendungen radikal zu erweitern und die Erträge in Ihrem Unternehmen zu erhöhen.

Wir begannen damit, Ihnen zu zeigen, wie Sie Ihre On-Premises-Anwendungen mit Funktionen und Diensten der Cloud wie z. B. Sichern und Wiederherstellen, Disaster Recovery und Anwendungsintegration nutzen können.

In Kapitel 11 sahen wir uns im Detail die neuen verfügbaren Anwendungsmodelle in der Cloud an, einschließlich PaaS und Container. Dank der serverlosen Funktionen können Ihre Teams neue Anwendungen erstellen, ohne auch nur eine Codezeile zu schreiben.

Als Dienste stehen Ihnen ebenfalls eine ganze Menge Datenverwaltungstools in der Cloud zur Verfügung: nicht nur relationale Datenbanken und Data Warehouses, sondern auch Dokumentendatenbanken, Big Data Repositories wie Hadoop und Spark sowie Analysedienste.

Schließlich zeigten wir in Kapitel 13, wie die neuen Welten von künstlicher Intelligenz und Machine Learning auf Anhieb kostengünstige transformative Vorteile für Ihre Anwendungen und Geschäfte bieten können, und zwar durch Funktionen wie Bots und eine prädikative Wartung.

* * *

Wir sind der Meinung, dass die Cloud ganz allgemein eine unglaublich spannende Chance für IT-Organisationen und Unternehmen darstellt. Wir hoffen, dass Sie durch das Lesen dieses Dokuments gelernt haben, wie Sie sämtliche Vorteile der Cloud schnell umsetzen können.

Viel Spaß auf Ihrer Reise in die Cloud!

Cloud- Architektur- Blueprints

Besuchen Sie die www.azure.com/solutions-Website, um die neuesten Blaupausen der Cloud-Lösungsarchitektur anzuzeigen. Einige davon befinden sich in diesem Anhang und verdeutlichen das Potenzial der Cloud-Architektur, das wir in diesem Buch erörtert haben.

Digitales Marketing

Einfache digitale Marketing-Website

Abbildung A-1 zeigt ein Beispiel für ein einfaches Content Management-System, mit dem Sie das Messaging auf Ihrer Website in Echtzeit über einen Browser und ohne jegliche Programmierkenntnisse verwalten können.

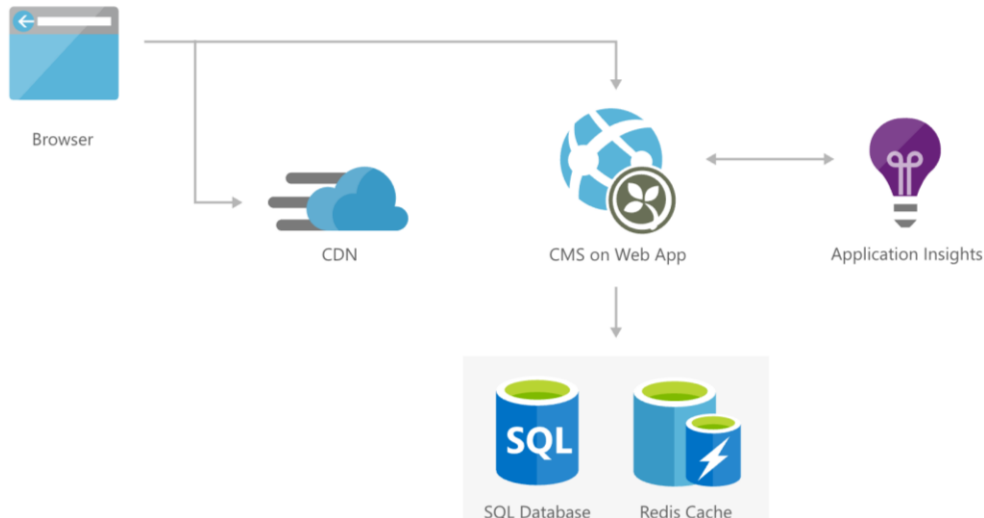


Abbildung A-1: Eine einfache digitale Marketing-Website

Diese Lösung wurde auf folgenden von Microsoft Azure verwalteten Diensten entwickelt:

- [SQL Database](#)
- [Application Insights](#)
- [Content Delivery Network](#)
- [Redis Cache](#)

Genau wie mit allen in diesem Anhang aufgeführten Dienstleistungen funktionieren sie in einer hochverfügbaren Umgebung, die gepatcht und unterstützt wird, und machen es für Sie möglich, sich auf Ihre Lösung auf die Umgebung zu konzentrieren, in der sie ausgeführt werden.

Skalierbare Umbraco CMS-Web-App

Eine größere Marketing-Website verwendet die Open-Source Umbraco Content Management-System-Webanwendung. Abbildung A-2 zeigt, dass sie skalierbar konfiguriert und für eine vielbesuchte Websites optimiert ist. Dabei werden zwei Web-Apps genutzt: eine für Ihre Front-End-App und die andere für Ihre Backoffice-App, die in einer einzelnen Region ausgeführt wird und die automatische Skalierung aktiviert hat.

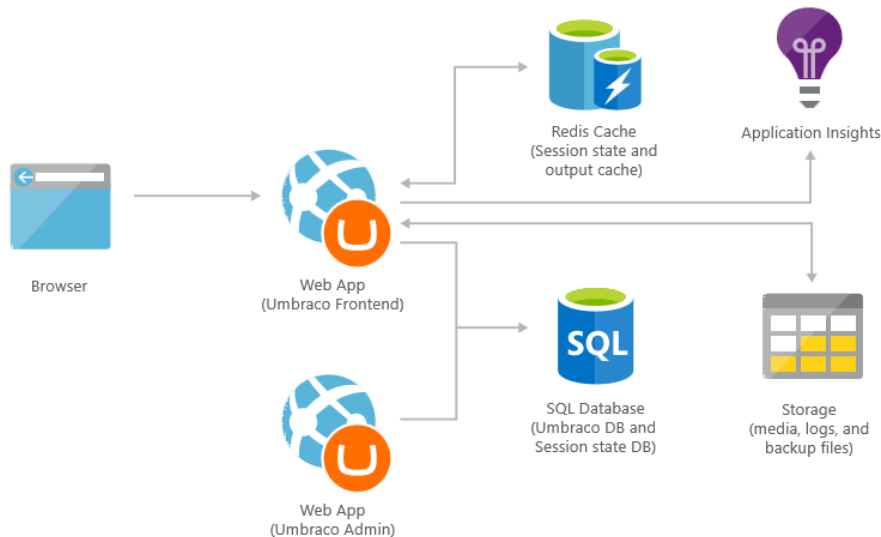


Abbildung A-2: Skalierbare CMS-Web-App

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [SQL Database](#)
- [Speicher](#)
- [Application Insights](#)
- [Redis Cache](#)

Mobil

Aufgabenbasierte mobile App für Verbraucher

Abbildung A-3 zeigt ein Beispiel eines mobilen Back-Ends, das von iOS-, Android- und Windows-Clientapps verwendet wird. Sie können Xamarin oder native Client-SDKs verwenden, um eine mobile Clientapp mit Unterstützung für Offlinesynchronisierung zu entwickeln, einschließlich der Offlinesynchronisierung von Bilddateien. Die App Service-Authentifizierung wird verwendet, um die Verbindung mit einem Identity-Provider herzustellen. Azure Blob Speicher wird verwendet, um Bilder auf kostengünstige und skalierbare Weise zu speichern.

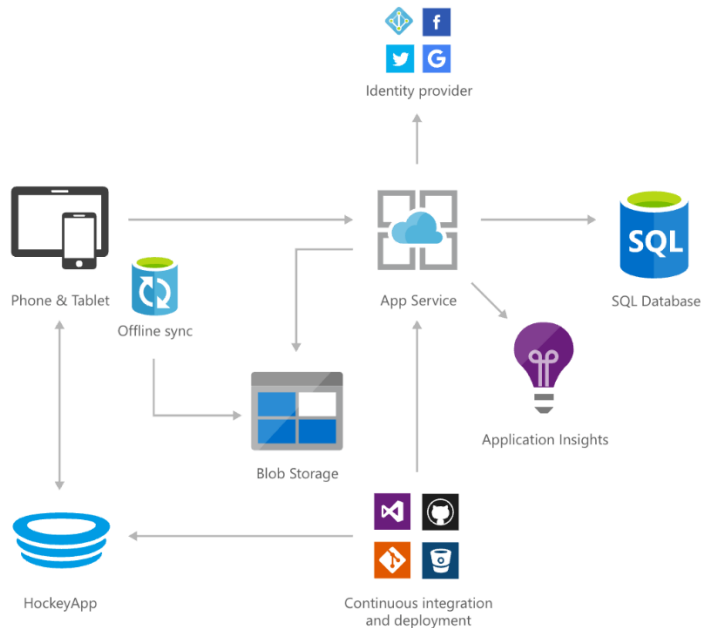


Abbildung A-3: Aufgabenbasierte mobile App für Verbraucher

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [App Service](#)
- [SQL Database](#)
- [Application Insights](#)
- [HockeyApp](#)

Benutzerdefinierte mobile App für Mitarbeiter

In diesem Beispiel (Abbildung A-4) funktioniert eine Xamarin.Forms-Clientapp mit Support für iOS, Android und Windows Offline und ermöglicht den Technikern vor Ort, die ihnen zugewiesenen Aufträge einzusehen und zu bearbeiten.

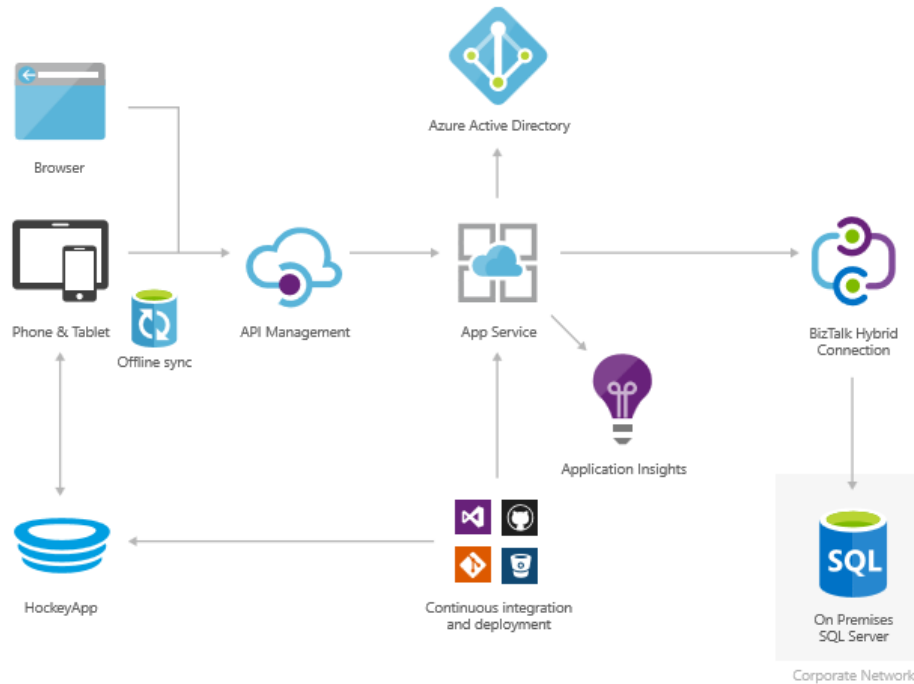


Abbildung A-4: Benutzerdefinierte mobile App für Mitarbeiter

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [App Service](#)
- [API Management](#)
- [SQL Database](#)
- [Azure Active Directory](#)
- [Application Insights](#)
- [HockeyApp](#)

Soziale mobile und Web-App mit Authentifizierung

Abbildung A-5 zeigt eine mobile Client-App für das soziale Teilen von Bildern mit einer begleitenden Web-App. Das Backend der App übernimmt die Bildbearbeitung mit Azure Functions im Hintergrund. Die mobile Client-App funktioniert im Offlinemodus und ermöglicht Ihnen, Bilder anzuzeigen und hochzuladen, auch wenn Sie nicht über eine Netzwerkverbindung verfügen.

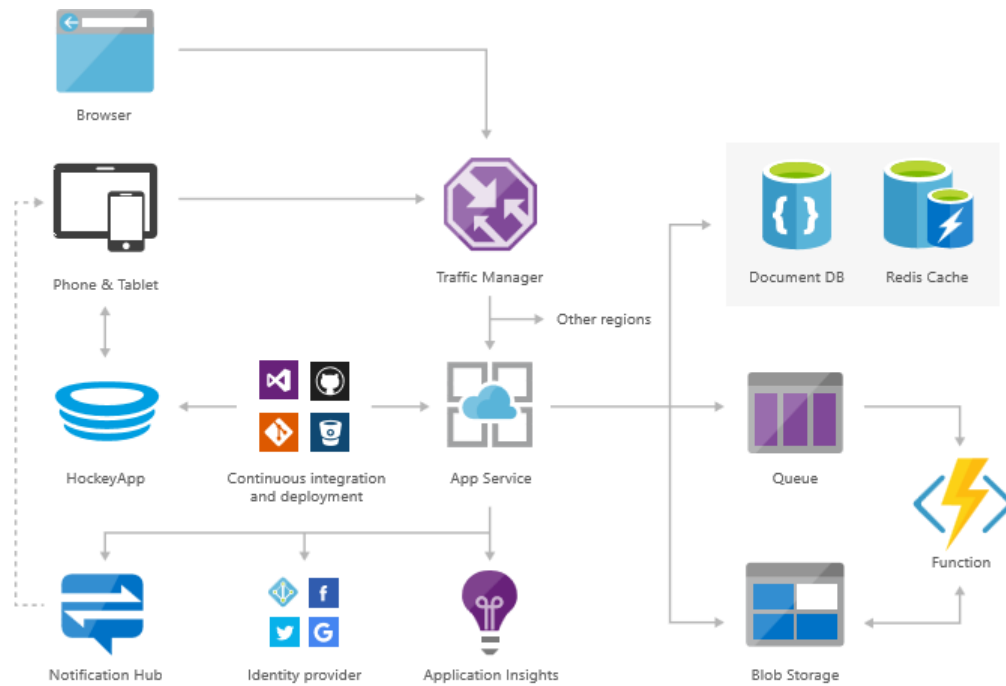


Abbildung A-5: Soziale mobile und Web-App mit Authentifizierung

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [App Service](#)
- [Traffic Manager](#)
- [Azure Cosmos DB](#)
- [Redis Cache](#)
- [Notification Hubs](#)
- [Azure Active Directory](#)
- [Functions](#)
- [Application Insights](#)
- [HockeyApp](#)

Backup und Archivierung

Abbildung A-6 veranschaulicht, wie Daten und Anwendungen von einem On-Premises-System auf Azure mit Azure Backup oder einer Partnerlösung gesichert werden. Eine Internetverbindung mit Azure dient zum Herstellen der Verbindung mit Azure Backup oder Azure Blob Speicher. Der Azure Backup-Server kann Backups direkt auf Azure Backup schreiben. Alternativ kann eine Partnerlösung wie Commvault Simpana oder Veeam Availability Suite, die On-Premises gehostet sind, die Backups direkt auf Blob Speicher oder über einen Cloud-Endpunkt wie Veeam Cloud Connect schreiben.

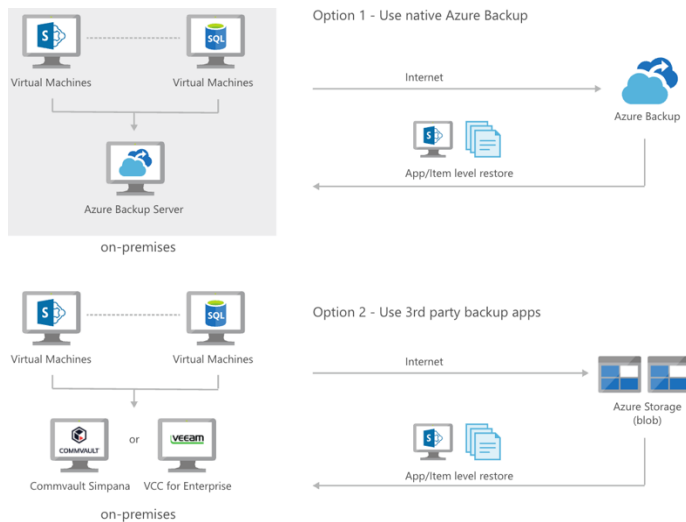


Abbildung A-6: Backup und Archivierung

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Backup Server](#)
- [Backup](#)
- [Blob Speicher](#)

Entwicklung und Test

Entwicklung und Test für IaaS

Abbildung A-7 zeigt, wie Sie Ihre Infrastruktur für die Entwicklung und das Testen eines Standard-IaaS-basierten SaaS-Systems konfigurieren.

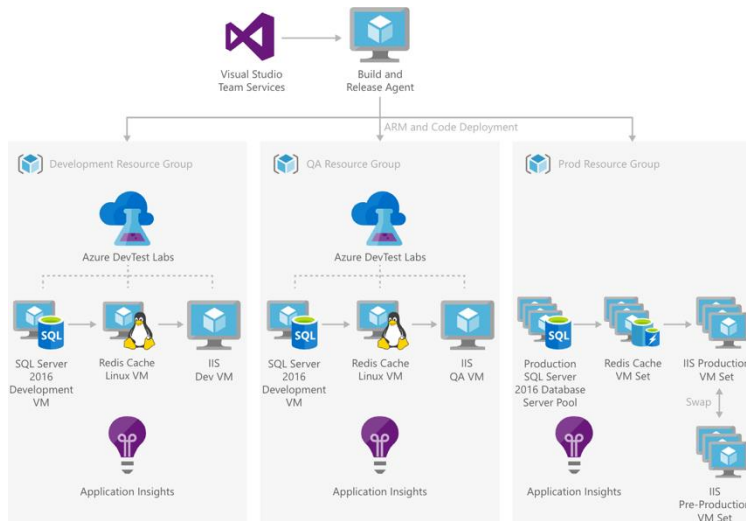


Abbildung A-7: Entwicklung und Test für IaaS

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Visual Studio Team Services](#)
- [Azure DevTest Labs](#)
- [Virtuelle Maschinen](#)
- [Application Insights](#)

Entwicklung und Test für PaaS

Abbildung A-8 zeigt, wie Sie Ihre Infrastruktur für die Entwicklung und das Testen eines Standardsystems im PaaS-Stil konfigurieren.

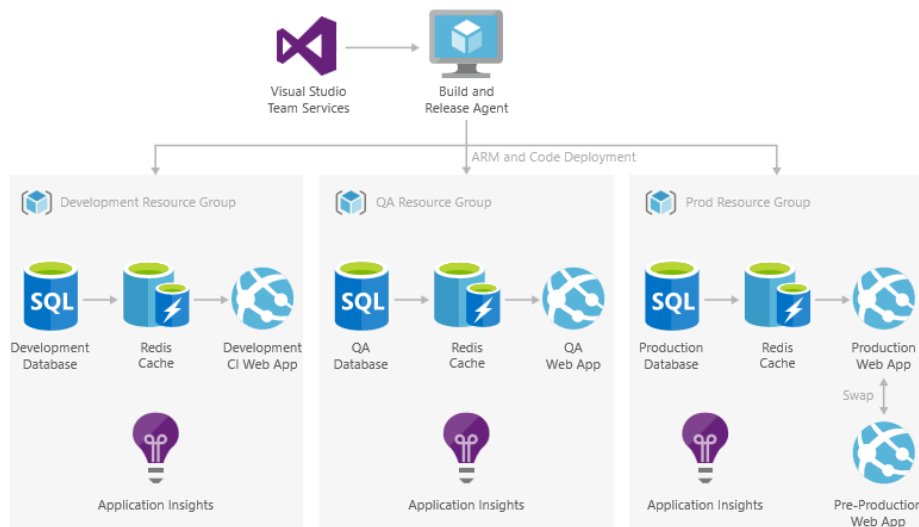


Abbildung A-8: Entwicklung und Test für PaaS

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Visual Studio Team Services](#)
- [SQL Database](#)
- [Redis Cache](#)
- [Application Insights](#)

Entwicklung und Test für Microservices-Lösungen

Abbildung A-9 zeigt wie Sie Ihre Infrastruktur für die Entwicklung und das Testen eines Microservices-basierten Systems konfigurieren.

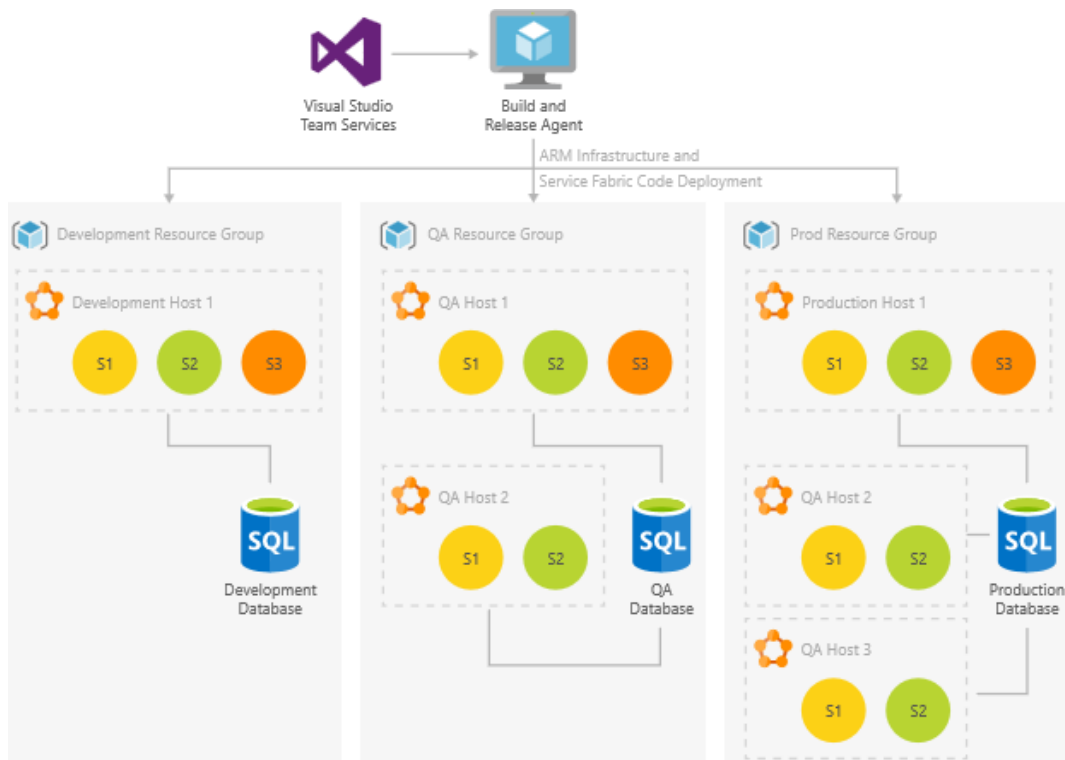


Abbildung A-9: Entwicklung und Test für Microservices-Lösungen

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Visual Studio Team Services](#)
- [Service Fabric](#)
- [SQL Database](#)

Notfallwiederherstellung

Unternehmensweite Notfallwiederherstellung

Abbildung A-10 zeigt eine große Enterprise-Architektur für Microsoft SharePoint, Dynamics CRM und Linux-Webserver, die in einem On-Premises-Rechenzentrum mit Failover zur Azure-Infrastruktur gehostet sind.

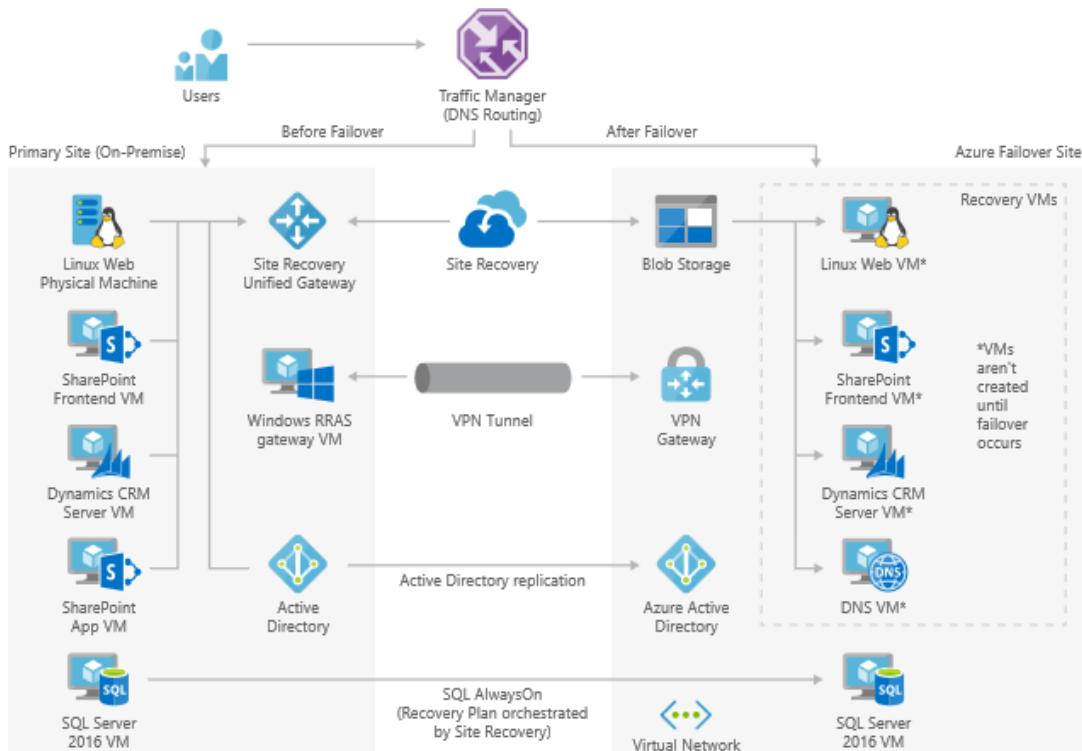


Abbildung A-10: Unternehmensweite Notfallwiederherstellung

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Traffic Manager](#)
- [Site Recovery](#)
- [Azure Active Directory](#)
- [VPN Gateway](#)
- [Virtual Network](#)

SMB-Notfallwiederherstellung mit Site Recovery in Azure

Sie können in kleinen und mittelständischen Unternehmen Notfallwiederherstellungen kostengünstig mit Azure Site Recovery oder einer Partnerlösung wie Double-Take DR in der Cloud implementieren. Figur A-11 veranschaulicht die Site Recovery-Lösung.

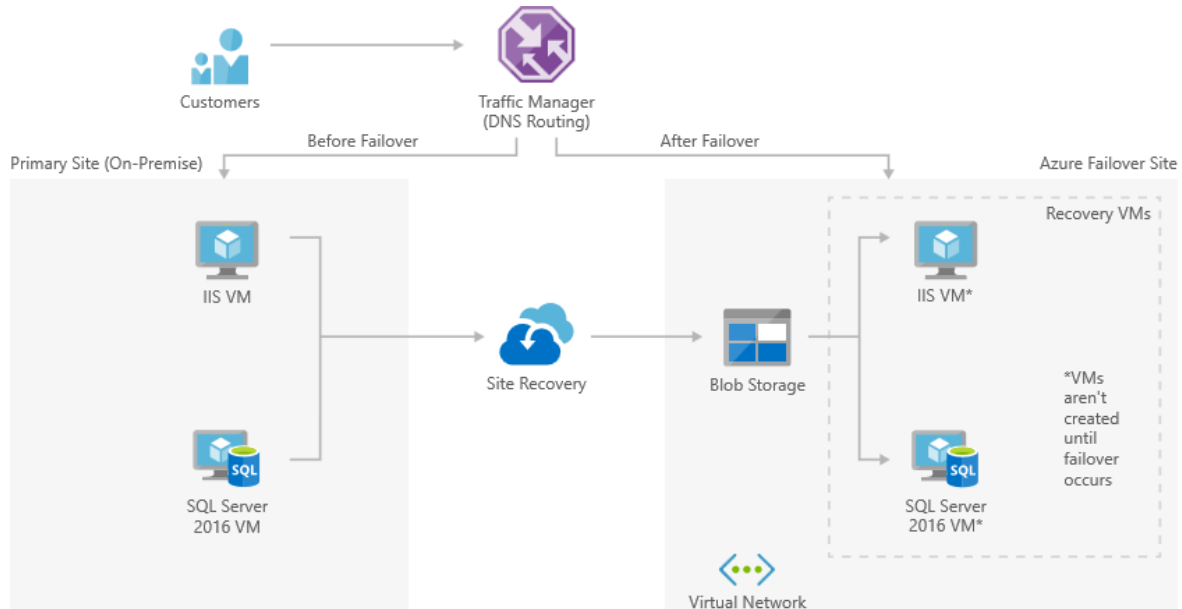


Abbildung A-11: SMB-Notfallwiederherstellung mit Azure Site Recovery

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Traffic Manager](#)
- [Site Recovery](#)
- [Virtual Network](#)

SAP auf Azure

SAP HANA für Azure

Die in Abbildung A-12 dargestellte Architektur stellt ein verteiltes dreistufiges SAP System dar, das auf einem SQL Server in der Azure Cloud Platform ausgeführt wird.

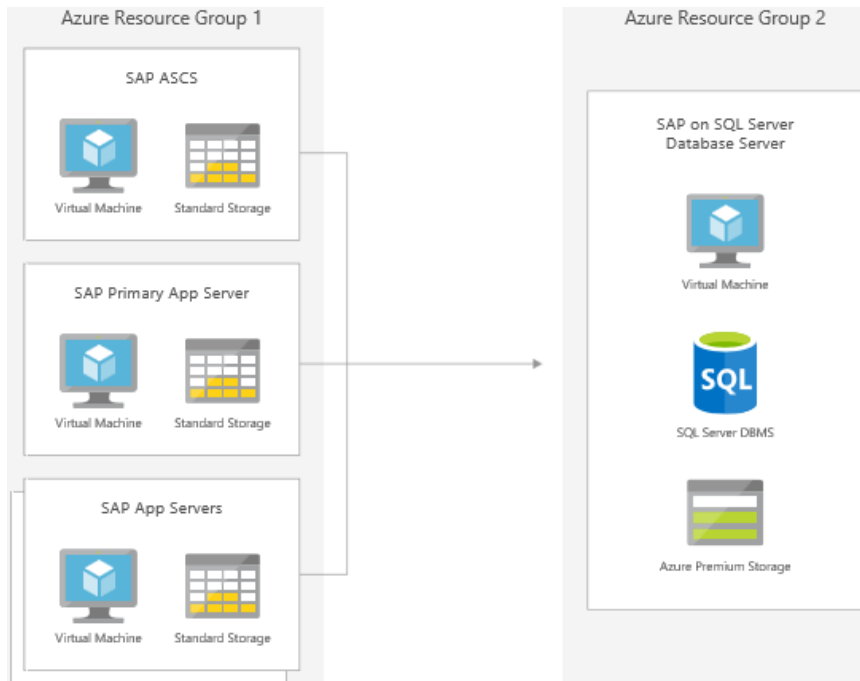


Abbildung A-12: SAP Hana für Azure

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Virtuelle Maschine](#)
- [Speicher](#)

SAP Hana auf Azure Architektur (große Instanz)

Das Diagramm in Abbildung A-13 veranschaulicht, wie Sie Ihre Infrastruktur konfigurieren, um SAP HANA auf Azure auszuführen (große Instanz). Dies umfasst die Anwendungsebene in einem Rechenzentrum für Azure und HANA in einem Rechenzentrum mit großer Instanz.

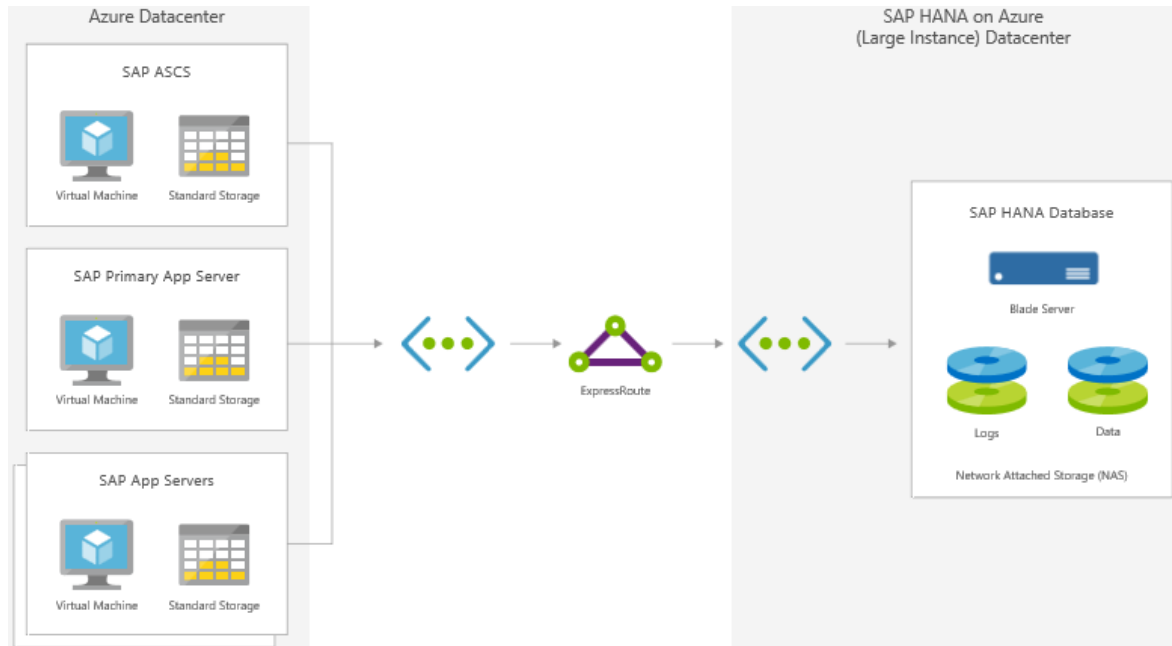


Abbildung A-13: SAP Hana für Azure (große Instanz)

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Virtuelle Maschine](#)
- [Speicher](#)
- [ExpressRoute](#)
- [Virtual Network](#)

Hochleistungs-Computing

Big Compute-Lösungen als Service

Hochleistungs-Computing-Anwendungen (HPC) können Tausende von Prozessorkernen skalieren, On-Premises Big Compute erweitern oder als 100 Prozent Cloud-Native Lösung ausgeführt werden. Die in Abbildung A-14 gezeigte HPC-Lösung wird mithilfe von Azure Batch implementiert, das eine Arbeitsplanung, eine automatische Skalierung der Computeressourcen und Execution Management als Plattformdienst (PaaS) anbietet, um den HPC-Infrastruktur-Code und die Wartung zu reduzieren.

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Virtuelle Maschine](#)
- [Speicher](#)
- [Batch](#)

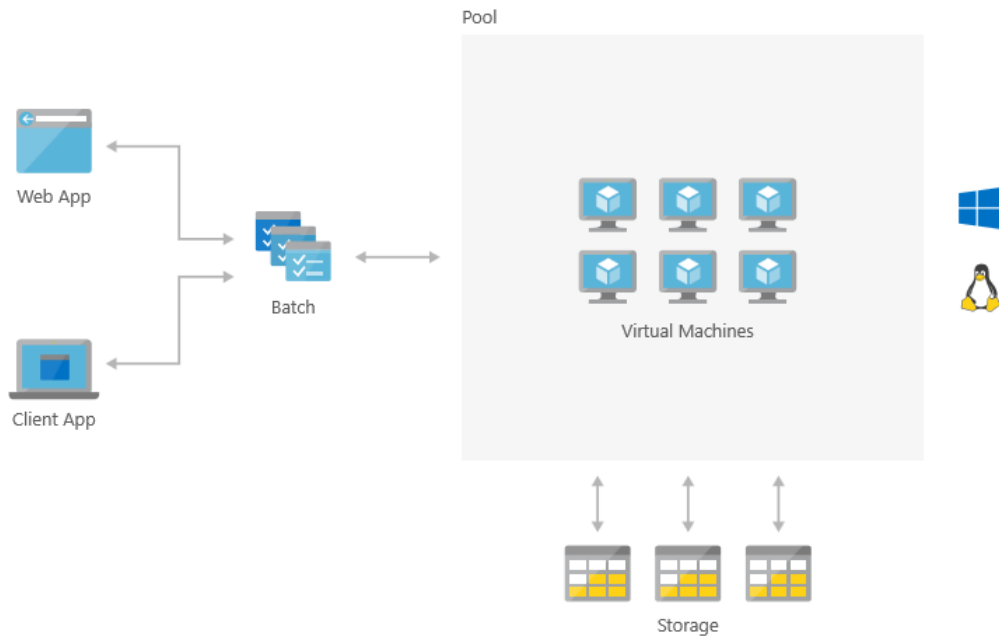


Abbildung A-14: Big Compute-Lösungen als Service

In der Cloud bereitgestellte HPC-Cluster

Die in Abbildung A-15 angezeigte HPC-Lösung umfasst die Hauptknoten, Serverknoten und Speicherknoten und funktioniert in Azure ohne Wartung der Hardwareinfrastruktur.

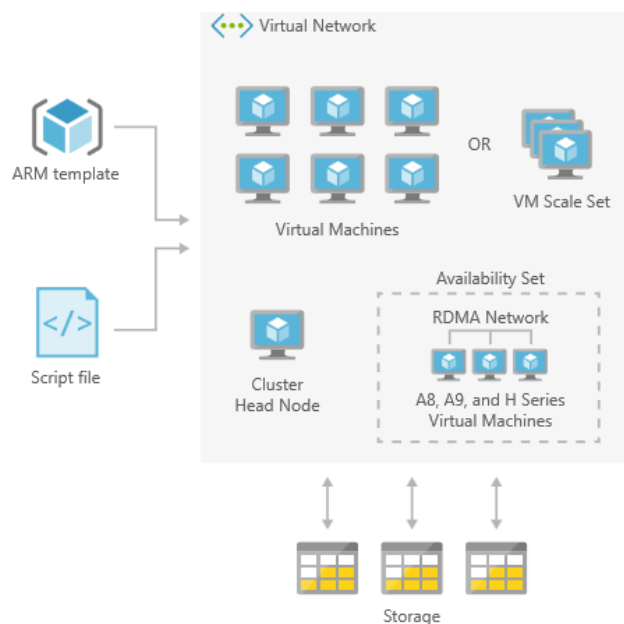


Abbildung A-15: In der Cloud bereitgestellte HPC-Cluster

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Virtual Machine Scale Sets](#)
- [Virtual Network](#)
- [Speicher](#)

On-Premises-HPC-Implementierung auf Azure laden

Eine HPC-Lösung kann außerdem die Rechenkapazität durch Erweitern der rechenintensiven Instanzen von virtuellen Maschinen in Azure erweitern und ist über Express Route oder VPN zugänglich, wie in Abbildung A-16 dargestellt.

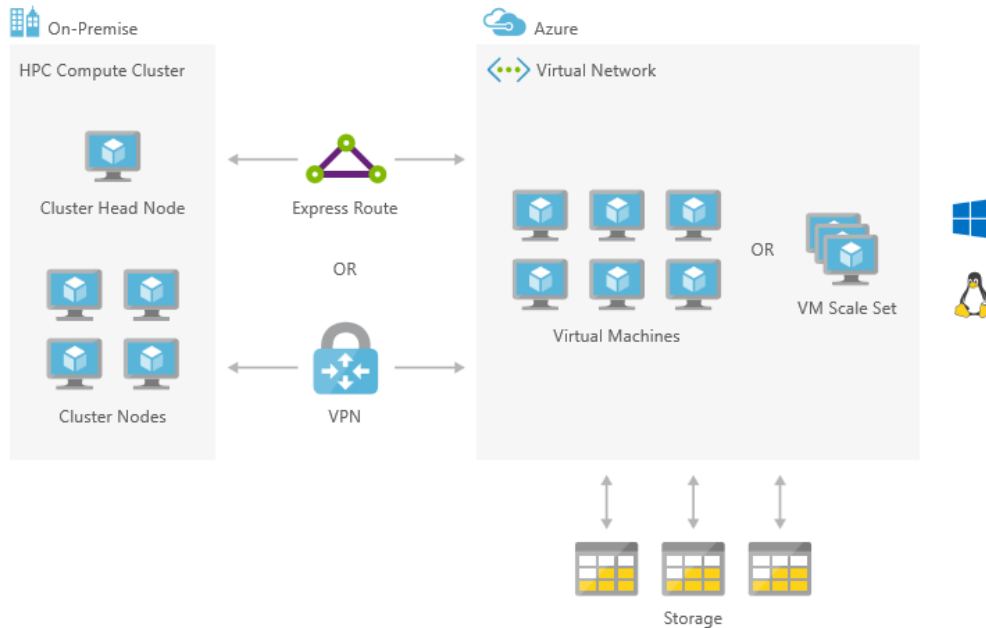


Abbildung A-16: On-Premises-HPC-Implementierung auf Azure laden

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Virtuelle Maschine](#)
- [Virtual Network](#)
- [VPN Gateway](#)
- [ExpressRoute](#)
- [Speicher](#)

Digitale Medien

Digitale Medien: Video-on-Demand

Abbildung A-17 zeigt grundlegende Video-on-Demand-Lösung, mit denen Sie aufgezeichnete Video-Inhalte wie Filme, Nachrichten-Clips, Sportsegmente, Schulungsvideos und Kundendienst-Tutorials auf videofähigen Endpunkt-Geräten, mobilen Anwendungen oder Desktop-Browsern wiedergeben können. Video-Dateien werden auf den Azure Blobpeicher hochgeladen, in ein Multi-Bitraten-Standardformat kodiert und dann über alle wesentlichen adaptiven Bitrate-Streaming-Protokolle (HLS, MPEG-DASH, Smooth) auf dem Azure Media Player-Client verteilt.

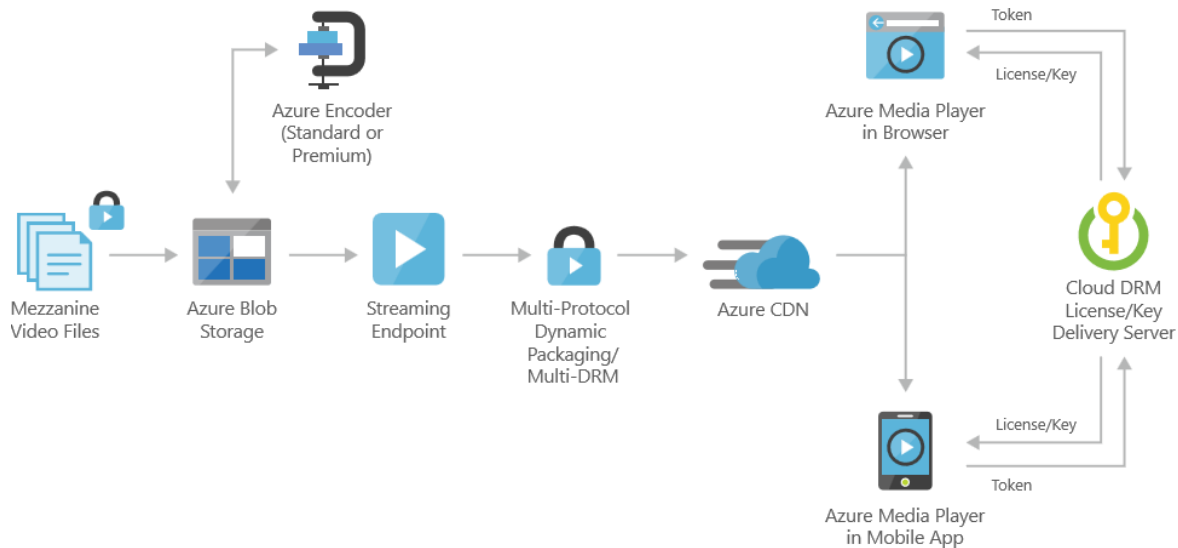


Abbildung A-17: Digitale Medien: Video-on-Demand

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Blob Speicher](#)
- [Content Delivery Network](#)
- [Azure Media Player](#)

Digitale Medien: Livestreaming

Eine Livestreaming-Lösung ermöglicht Ihnen, Videos in Echtzeit zu erfassen und für die Verbraucher in Echtzeit wiederzugeben. Dabei handelt es sich zum Beispiel um das Onlinestreaming von Interviews, Konferenzen und Sportveranstaltungen. In der in Abbildung A-18 dargestellten Lösung wird das Video von einer Videokamera erfasst und an den Endpunkt des Eingabekanals gesendet. Der Kanal erhält die Liveaufnahme in der Eingabe und stellt sie für das Streaming über einen Streaming-Endpoint in einen Webbrowser oder über eine mobile App zur Verfügung. Der Kanal bietet ebenfalls einen Vorschau-Überwachungsendpunkt, um die Vorschau und Ihren Stream vor einer weiteren Verarbeitung und Lieferung zu überprüfen. Der Kanal kann außerdem die erfassten Inhalte aufzeichnen und speichern, um diese später (Video-on-Demand) zu streamen.

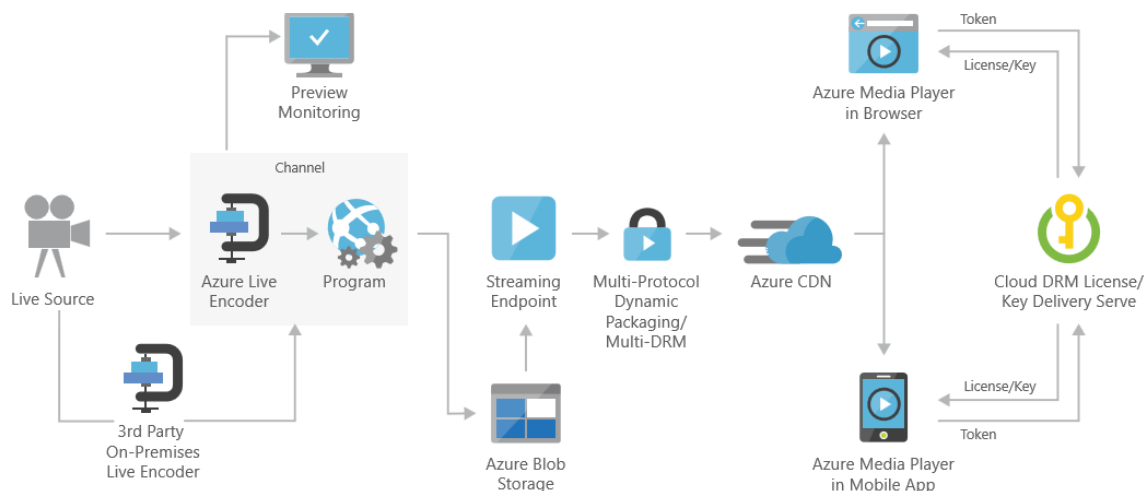


Abbildung A-18: Digitale Medien: Livestreaming

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Media Services](#)
- [Content Delivery Network](#)

Schlagwortsuche/Spracherkennung/optische Bilderkennung bei digitalen Medien

Sie können mit einer Spracherkennungslösung die Sprache in statischen Videodateien identifizieren, damit diese als Standardinhalt verwaltet werden kann, z. B. um es Angestellten zu ermöglichen, in Schulungsvideos nach gesprochenen Worten oder Sätzen zu suchen und anschließend schnell an die bestimmte Stelle im Video zu navigieren. Die Lösung in Abbildung A-19 ermöglicht Ihnen, statische Videos auf eine Azure-Website hochzuladen. Der Azure Media Indexer verwendet die Sprach-API, um die Sprache innerhalb der Videos zu indizieren und sie in SQL Azure zu speichern. Sie können mit Azure Web Apps nach Wörtern oder Sätzen suchen und eine Liste der Ergebnisse abrufen. Wenn Sie ein Ergebnis auswählen, wird angezeigt, wo das im Video erwähnte Wort oder der Ausdruck auftaucht.

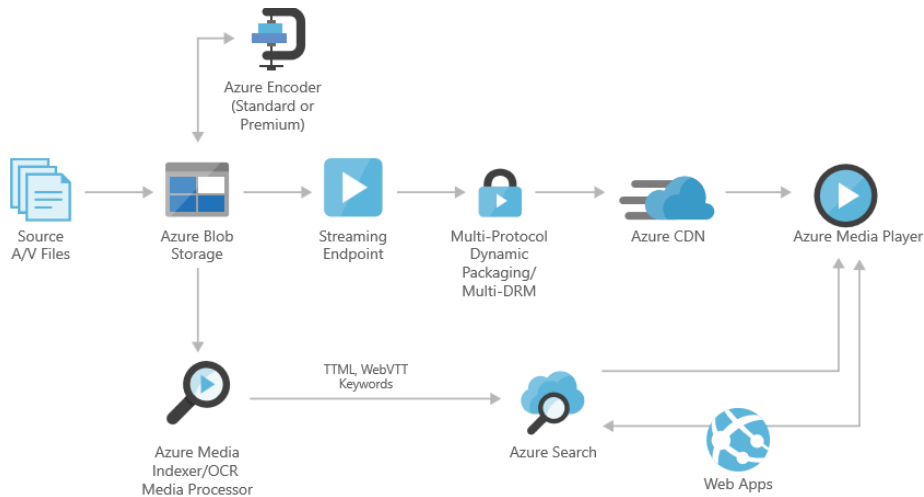


Abbildung A-19: Digitale Medien: Video-on-Demand

Diese Lösung wurde auf folgenden von Azure verwalteten Diensten entwickelt:

- [Content Delivery Network](#)
- [Azure Search](#)

E-Commerce

Bevor Sie etwas verkaufen können, muss dafür eine Nachfrage bestehen. Mit der E-Commerce-Plattform von Microsoft können Sie den Website-Traffic und die Suche von Abschlussraten für den Kauf analysieren, um spezielle Angebote und neue Produkte basierend auf dem Verhalten der Kunden zu bestimmen. Erstellen Sie personalisierte Einkaufserlebnisse mit gezielten Inhalten und Angeboten, und steigern Sie die Zufriedenheit durch ein anhaltendes Engagement – vor, nach und während dem Verkauf.

Mehr Kunden bedeuten mehr Transaktionen. Stellen Sie sicher, dass Sie jede Transaktion reibungslos durchführen können, indem Sie ein E-Commerce-Einkaufserlebnis entwerfen, das sich ganz einfach navigieren lässt. Stellen Sie es anschließend auf einer sicheren und konformen E-Commerce-Plattform bereit.

Ihre E-Commerce-Lösung sollte sich der Größe und der Saisonabhängigkeit Ihres Unternehmens anpassen. Wenn die Nachfrage nach Ihren Produkten oder Dienstleistungen boomt – vorhersehbar oder unvorhersehbar – sollten Sie bereit sein, mehr Kunden und mehr Transaktionen automatisch zu verarbeiten. Profitieren Sie darüber hinaus von der Cloud-Wirtschaftlichkeit und zahlen Sie nur für die Kapazität, die Sie auch tatsächlich verwenden.

Ihr Kerngeschäft ist der Verkauf von Produkten und nicht, eine IT-Organisation zu führen. Nutzen Sie die vorgefertigten Dienste, wie die in Abbildung A-20 gezeigten Dienste in der Cloud, um eine E-Commerce-Lösung zu entwickeln, die Ihre Vertriebsleistung erhöht und die Verwaltung der Infrastruktur Ihrem Cloud-Anbieter überlässt.

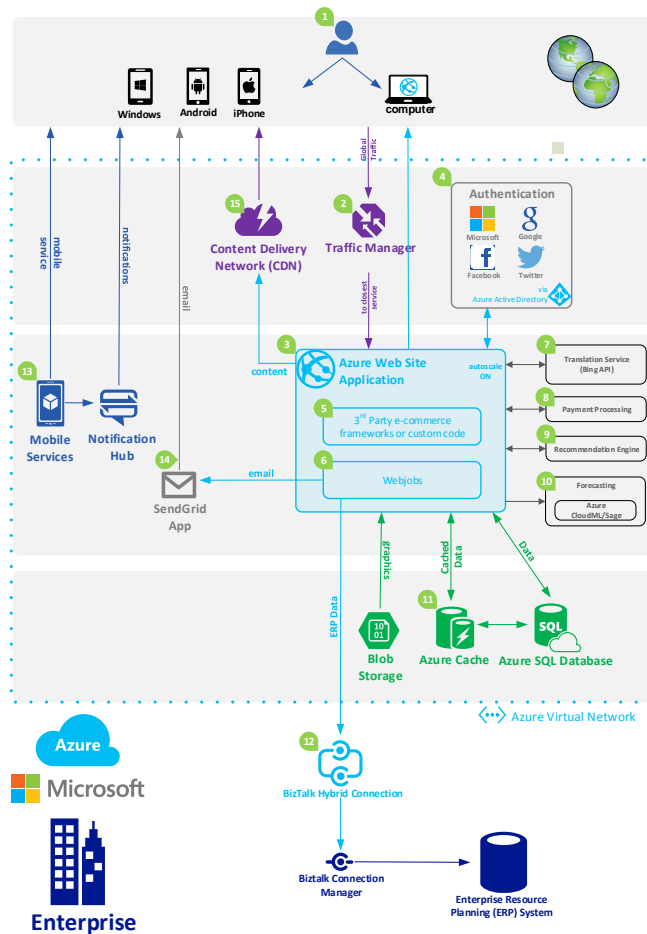


Abbildung A-20: E-Commerce-Lösung

Wie in der Abbildung gezeigt:

1. Benutzer durchsuchen und bestellen Artikel über Telefone, Tablets und PCs mit HTML oder systemeigenen Anwendungen.
2. Stellen Sie es in mehreren Rechenzentren zur globalen Skalierung bereit und verwenden Sie Azure Traffic Manager zur Weiterleitung von Anfragen an das nächstgelegene Rechenzentrum.
3. Azure Websites skaliert automatisch und verwaltet so Spitzen in den Einkaufsmustern der Kunden.
4. Benutzer melden sich mithilfe der Anmeldeinformationen von Facebook, Google, Microsoft, Twitter oder anderen Identitätsanbietern in Azure Active Directory an.

5. Sparen Sie Zeit, indem Sie kommerzielle Frameworks von Dritten oder Ihre eigenen verwenden.
6. WebJobs läuft im Hintergrund und übermittelt Aufträge an das On-Premises-Enterprise Resource Planning (ERP)-System und sendet Auftragsbestätigungen.
7. Erstellen Sie eine globale Website mithilfe des Übersetzungsdiensts von Bing.
8. Azure ist mit dem Payment Card Industry Data Security Standard (PCI DSS) für die Zahlungsverarbeitung konform.
9. Gezielte Artikelempfehlungen werden von einem Hadoop-basierten Empfehlungsmodul bereitgestellt.
10. Prognostizieren Sie die künftige Nachfrage nach Artikeln mithilfe von Cloud Machine Learning.
11. Azure Cache steigert die Leistung aller Datendienste.
12. Verwenden Sie Azure Hybrid Connections zum Senden von Nachrichten an On-Premises-Datenbanken.
13. Azure Mobile Services bietet ein einheitliches Back-End für mobile Bestellungen, einschließlich Geräteauthentifizierung, Datendienste und Benachrichtigungen.
14. Senden Sie E-Commerce-Bestätigungen mithilfe einer Drittanbieter-App.
15. CDN an verschiedenen geografischen Standorten bewahrt die Video- und Grafikressourcen näher bei den Benutzern auf.

Der Azure Marketplace bietet zurzeit viele vorgefertigte E-Commerce-Lösungen, inklusive OpenCart, Virtocommerce, AbanteCart und NopCommerce.

Internet der Dinge

Mithilfe des Azure IoT Hub können Sie unglaubliche Mengen (Milliarden) an Internet der Dinge (IoT)-Geräten sicher miteinander verbinden. Und genau wie für alle Dienste in der Cloud, zahlen Sie nur für das, was Sie auch tatsächlich nutzen. Der IoT Hub und seine Softwareentwicklungs-Kits für Windows, Linux und Echtzeit-Betriebssysteme (RTOS) unterstützen eine Vielzahl an Protokollen, einschließlich Representational State Transfer (REST), Advanced Message Queuing Support (AMQP) und MQTT Telemetry Support (MQTT). Die Sicherheit steht Ihnen durch die optionale Authentifizierung pro Gerät und die verschlüsselte Kommunikation zur Verfügung.

Ziehen Sie für Anwendungen, die Entscheidungen in Echtzeit treffen, und künstliche Intelligenz, die sich auf Ihren IoT-Geräten vor Ort befindet, den neuen IoT Edge-Dienst in Betracht. Dieser richtet künstliche Intelligenz, Analytics und eine Vielzahl von anderen Funktionen auf Ihrem IoT-Netzwerk ein.

Sie können ungenutzte Daten sammeln und prädiktive Modelle erstellen, wenn Sie eine Verbindung von Ihren Geräten, Anlagen und Sensoren mit der Cloud herstellen – von ein paar Sensoren bis zu Millionen von Geräten. Durch den Zugang zu Daten zur globalen Produktions- und Supply-Chain können Sie kostenintensive Ausfallzeiten und Wartung reduzieren und die Effizienz steigern.

Sie können sich auf das konzentrieren, was für Ihre Kunden von Bedeutung ist: Zuverlässigkeit. Verbessern Sie Prozesse und die Verfügbarkeit Ihrer Anlagen durch eine vorausschauende und sogar präventive Wartung, indem Sie Daten von Sensoren und Systemen sammeln und umwandeln.

Verbessern Sie die Sicherheit Ihrer physischen Geräte, Verbindungen und Daten. Verwenden Sie eine Authentifizierung pro Gerät durch die Einrichtung von individuellen IDs und Anmeldeinformationen für jedes Ihrer angeschlossenen Geräte und wahren Sie die Vertraulichkeit der C2D- und D2C-Nachrichten.

Wenden Sie mögliche Probleme ab, während Sie die Effizienz der Arbeitsgeräte durch eine vorausschauende Wartung verbessern. Sammeln und analysieren Sie die Daten aus Ihren vernetzten Ressourcen, um die Wartung proaktiv zu planen, Ausfallzeiten zu verringern und den Aufbewahrungswert Ihrer Ressourcen zu verbessern.

Beginnen Sie die Innovation noch heute mit IoT-Starterkits von Adafruit, Seeed und SparkFun, die Entwicklungsboards mit Azure-Zertifizierung für IoT anbieten.

Microservices-Anwendungen

In Kapitel 12 erläuterten wir Anwendungen, die auf dem Microservices-Modell basieren. Mit Azure Service Fabric und Azure Container Service können Sie die Skalierung, die Macht und die globale Reichweite erzielen, die Ihre Startup benötigt, um die Bedürfnisse Ihrer Kunden zu erfüllen, wenn Ihr Unternehmen wächst – ohne Ihre Anwendungen neu zu gestalten. Führen Sie Ihre Apps in der Skalierbarkeit der Cloud mit einer Vielzahl von Dienstleistungen aus, die es Ihnen ermöglichen, Ihre Energie auf die Entwicklung der Anwendungen anstatt der Verwaltung der Infrastruktur zu konzentrieren.

Mit den Microservices-Architekturen können Sie eine Aktualisierung in Echtzeit durchführen, während kleine Entwicklungsteams unabhängig voneinander arbeiten und kontinuierlich Pipelines und parallele Upgrades nutzen, damit sichergestellt wird, dass Ihre Kunden immer Zugriff auf die neuesten Funktionen haben.

Business Intelligence

Wie in Kapitel 12 schon angesprochen, ermöglicht Ihnen die Cloud große Mengen an Daten zu sammeln, analysieren und visualisieren. Mit Azure SQL Data Warehouse und Azure Analysis Services können Sie Business-Analysten – sowie jeder Person in Ihrem Unternehmen – leistungsstarke Tools zur Analyse und Business Intelligence (BI) anbieten, um bessere und schnellere Entscheidungen zu treffen. Kombinieren Sie Daten aus mehreren Quellen, um maßgeschneiderte Bericht und umfassende Analytics zu entwickeln, die Ihre Daten zum Leben erwecken.

Sie können darüber hinaus mit Microsoft Power BI eine atemberaubende Visualisierungen Ihrer Daten erstellen. Bei Microsoft gibt es eine Reihe vorgefertigter Power BI-Lösungsvorlagen auf der [Azure-Website](#).

Big Data und Analytics

Wie wir schon so oft in diesem Handbuch erklärt haben, steigt das Datenvolumen explosionsartig – von traditionellen POS-Systemen und E-Commerce-Websites zu neuen Kundensensorquellen wie Twitter und IoT-Sensoren, die Daten in Echtzeit mit Apache Hadoop und Spark streamen. Wenn Sie vielfältige Daten von Anfang an analysieren, treffen Sie fundierte Entscheidungen, die vorausschauend und ganzheitlich anstatt reaktiv und getrennt sind. Sie können die Daten Ihrer Organisation auf unbestimmte Zeit behalten, und zwar unabhängig von der Größe. Anstatt Kompromisse bei den Kosten einzugehen, welche Daten Sie behalten sollen, können Sie Ihre Daten speichern und so die Einhaltung von Richtlinien und Unternehmensstandards zu erschwinglichen Preisen erfüllen – das ist jetzt mit der Hadoop- und Spark- Technologie in der Cloud möglich.

Azure HDInsight bietet einen verwalteten Hadoop-, Spark, R Server-, HBase- und Storm-Dienst an. Data Lake Analytics bietet massiv skalierbare analytische Dienstleistungen an – Sie können natürlich diese und andere Tools von anderen Anbietern (wie Cloudera, Databricks und Informatica) mit den Machine Learning-Funktionen von Azure verwenden.

Cloud-Migration

Neben den in diesem Buch angebotenen Tipps bietet Azure eine Reihe von Tools an, die Ihnen bei der Cloud-Migration helfen.

Wie bereits erwähnt, sollten Sie Azure Site Recovery in Erwägung ziehen, um die physische Migration von virtuellen Maschinen (VMs) von On-Premises-Infrastrukturen zur Cloud zu organisieren. Sie können ebenfalls Azure Site Recovery verwenden, um Anwendungen von einer Azure-Region auf die andere zu verlagern.

Nachdem Ihre Anwendungen in der Cloud sind, nutzt der Azure-Berater (Abbildung A-21) zieht auf Azure Best Practices, um Ihnen Lösungen anzubieten, die Ihre Kosten reduzieren und die Sicherheit, Leistung und Zuverlässigkeit Ihrer Anwendungen verbessern.

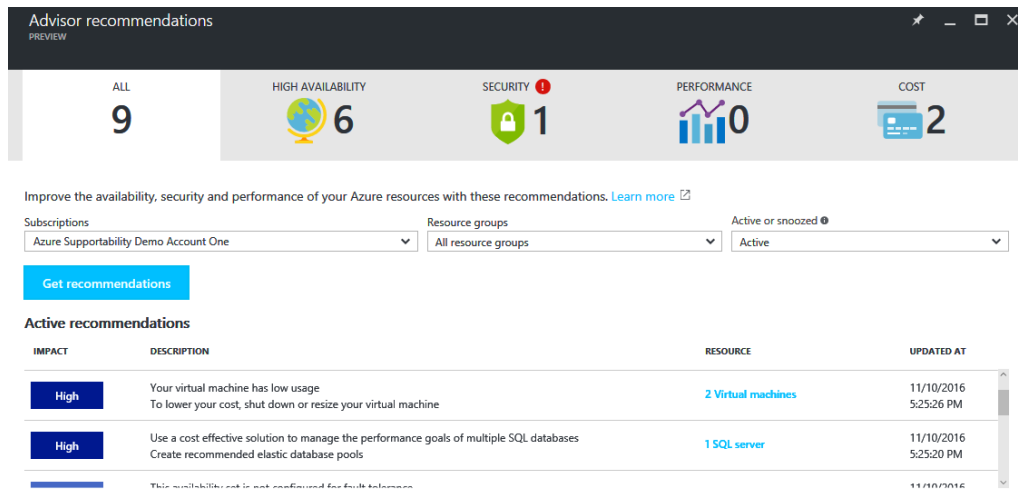


Abbildung A-21: Screenshot: Azur-Berater

Data Warehouse

Mit Azure SQL Data Warehouse können Sie Ihr Unternehmen durch vorausschauende Analytics aller Ihrer Daten mit Tools verändern, die Sie bereits kennen und lieben – Power BI, Microsoft Excel und BI-Tools von Drittanbietern. Darüber hinaus bietet die nahtlose Kompatibilität mit Machine Learning, Erfassung, Datentransfer und Datenspeicherdiensten transformative Einblicke über alle Ihre Daten.

SQL Data-Warehouse von Azure ist eine vollständig verwaltete Lösung, die innerhalb von Minuten bereitgestellt werden kann und – wie schon oft für andere Dienste betont wurde – flexibel skaliert und wobei Sie nur für das zahlen, was Sie nutzen.

Es gibt viele Datenmigrationstools, mit denen Sie Daten in ein Warehouse überführen können, einschließlich Azure Data Factory und Lösungen von CloudBeam, BlueTalon und SnapLogic. Diese stehen alle im Azure Marketplace zur Verfügung.

SaaS-Business-Apps

Möchten Sie Ihre eigene SaaS-Anwendung für den Einsatz in Ihrem Unternehmen oder zur Vermarktung an Ihre Kunden erstellen? Verwenden Sie die Azure SQL Database, um Daten in separaten Datenbanken zu isolieren und so eine konsistente Leistung und Datensicherheit zu gewährleisten – und zwar ohne zusätzliche Betriebs- oder Verwaltungskosten. Darüber hinaus können Sie die integrierte Angriffserkennung und Active Directory-Authentifizierung verwenden, um einen unbefugten Zugriff zu verhindern.

Sie erhalten auch vorhersehbare Kosten, um Ihr Geschäftsmodell sowie Einblicke in die Nutzungsmuster zu skalieren, wenn Ihr Unternehmen wächst. Mithilfe der verfügbaren Überwachungstools und Machine Learning können Sie die für Ihre SaaS-App erforderliche Betriebsumgebung erstellen.

Spiele

Einige der beliebtesten Onlinespiele, wie die von 343 Industries (Halo-Franchise), Next Games, Throwback, Illyriad, Io-Interactive und Xbox Studios, werden auf Azure ausgeführt.

Unabhängig von der Plattform, für die Sie die Spiele entwickeln – iOS, Android oder Windows – können Sie Azure nutzen, um die Back-End-Services der Spiele zu hosten, Push-Benachrichtigungen zu senden und die Analytics daten der Spiele zu verarbeiten und so das Benutzer-Engagement zu erhöhen.

Mit Azure können Sie die massiven Skalierungsanforderungen verwalten, die Ihre erfolgreichen Online und Social Games benötigen und gleichzeitig eine nahtlose Erfahrung für Gamer bereitstellen, ohne sich Sorgen über Ausfallzeiten oder Unterbrechungen machen zu müssen.

Sie können Ihre Spiele ruhigen Gewissens entwickeln und auf den Markt bringen. Verlassen Sie sich auf Microsoft und seine lange Tradition in puncto Entwicklung von AAA-Spielen für PC und Konsolen. Azure weitet dieses umfangreiche Wissen noch weiter aus und bietet der Entwicklung Ihrer Spiele Funktionen der Unternehmensklasse.

Sie können Mehrspieler-Szenarien und Leaderboards mit [Azure Active Directory](#) konfigurieren. Verwalten Sie die Spielerbeibehaltung, erhöhen Sie das Benutzer-Engagement und die Wertschöpfung auf allen Plattformen mit [Azure Notification Hubs](#) und [Azure Media Services](#). Mit den Notification Hubs können Sie personalisierte Pushbenachrichtigungen gezielt an einzelne Spieler oder ein ganzes Publikum mit Millionen von Benutzern auf allen ihren Geräten senden – einschließlich iOS, Android, Windows und Kindle. Mit Media Services haben Sie die Möglichkeit, Medienstreams zu verwalten und sogar Video-Werbungen in Ihre Spiele einzufügen.

Ob Sie über eine vorhandene Backend-Infrastruktur für ein Spiel verfügen oder Ihr System von Grund auf neu entwickeln möchten – Azure überlässt Ihnen die Wahl und Flexibilität. Verwenden Sie zum Heben und Verschieben Ihrer Infrastruktur in die Cloud IaaS-Angebote wie [virtuelle Maschine](#) und [virtuelle Maschine Scale Sets](#). Mit PaaS-Diensten wie [Azure Service Fabric](#) und [Azure App Service](#) können Sie sich auf die Entwicklung Ihrer Spiele konzentrieren und überlassen Azure die Verwaltung Ihrer Infrastruktur. Sie haben ebenfalls die Wahl zwischen verschiedenen Speicheroptionen, von verwalteten Datenbankdiensten wie Azure [SQL Database](#) und [Azure Cosmos DB](#) bis hin zu MongoDB, [Parse Server](#) und [DataStax Cassandra](#) auf [Azure Marketplace](#).

Blockchain

Blockchain ist eine neue Art und Weise für Unternehmen, Branchen und öffentliche Organisationen, Transaktionen beinahe sofort durchzuführen und zu überprüfen – so werden Geschäftsprozesse optimiert, Geld gespart und das Risiko von Betrug gesenkt. Im seinem Kern ist ein Blockchain eine Datenstruktur, die verwendet wird, um ein digitales Transaktionshauptbuch zu erstellen, das nicht nur von einem einzigen Anbieter sondern gemeinsam von einem Netzwerk an Computern genutzt wird.

Das Ergebnis ist ein offenes, transparentes und öffentlich nachweisbares System, das die uns bekannte Denkweise über den Austausch von Wert und Vermögenswerten grundlegend ändert, Verträge erzwingt und Daten innerhalb zahlreicher Branchen austauscht. Die Anwendungen, die Blockchain verwenden, sind nahezu unbegrenzt und reichen von Darlehen, Anleihen und Zahlungen über effiziente Lieferketten bis hin zur Identitätsverwaltung und -überprüfung.

Die im Azure Marketplace erhältliche Azure Blockchain-as-a-Service (BaaS) bietet schnelle, kostengünstige, risikoarme und FailFast-Plattformen für Organisationen, die durch das Experimentieren mit neuen Geschäftsprozessen zusammenarbeiten – die Technologie wird von einer Cloud Plattform mit dem größten Compliance-Portfolio in der Industrie unterstützt.

Serie von Geschäftsanwendungen

Wie in diesem Handbuch bereits angesprochen, können Sie jetzt Geschäftsanwendungen (LoB) ganz einfach auf Azure verschieben. Abbildung A-22 zeigt wie Sie die Kapazitäten von Azure am besten für IaaS VMs nutzen.

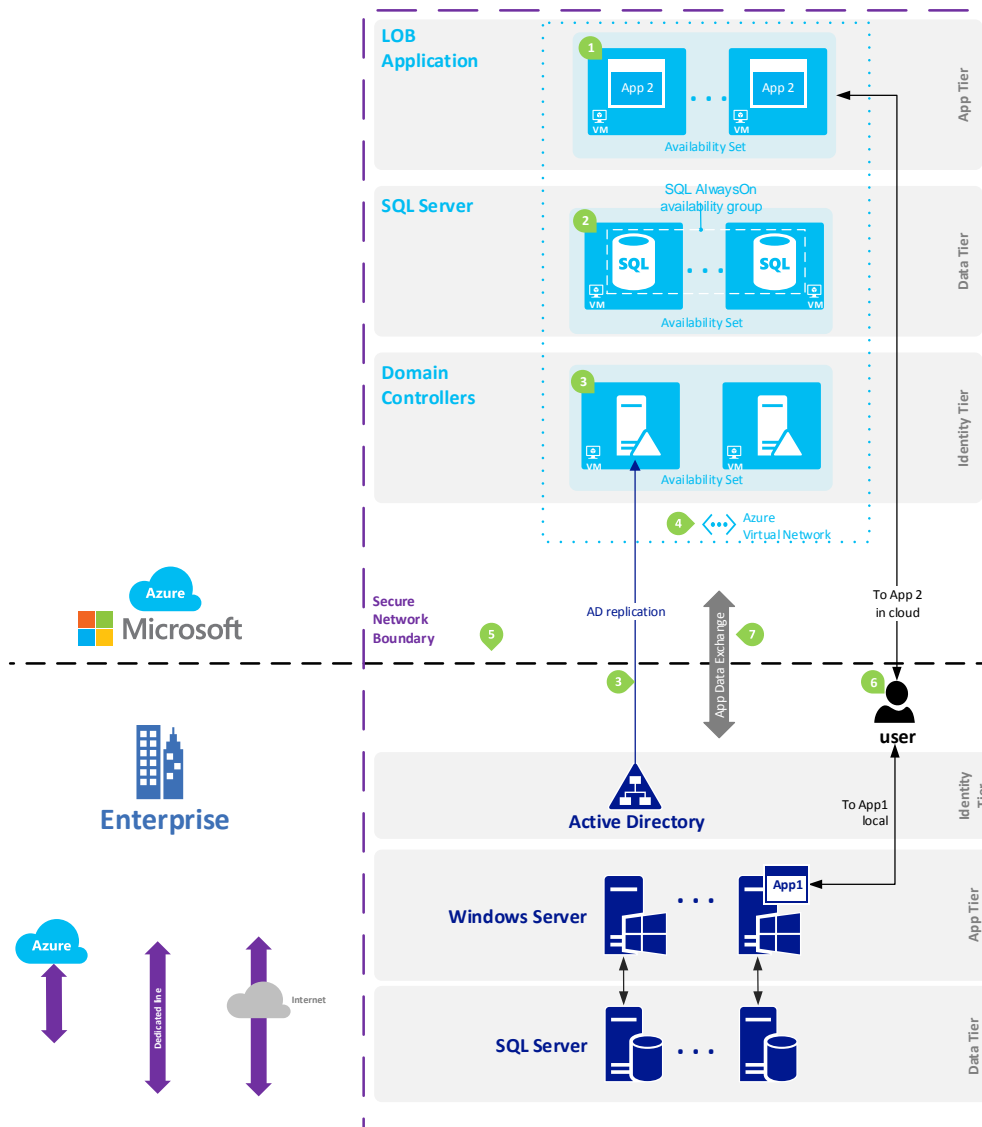


Abbildung A-22: Branchenanwendungen

Wie in der Abbildung gezeigt:

1. Packen Sie Ihre App auf eine virtuelle Maschine und stellen Sie sie in Azure bereit. Bewahren Sie mindestens zwei Kopien auf, um im Falle eines Ausfalls die Redundanz zu gewährleisten, und fügen Sie zum Skalieren weitere hinzu.
2. Verschieben Sie Ihre Datenebene in die Cloud, um die geringste Latenz zu ermöglichen. Nutzen Sie die SQL Server 2014 AlwaysOn-Funktion, um Redundanz und Failover bereitzustellen.
3. Führen Sie zwei VMs als Active Directory-Domänencontroller und DNS-Server in Azure aus und synchronisieren Sie diese Dienste mit Ihren On-Premises-Active Directory-Domänencontrollern. Die Anwendung kann anschließend Benutzer ohne die zusätzliche Latenz der Verbindung mit dem On-Premises-Active Directory authentifizieren.

4. Vernetzen Sie alle Ihre VMs in der Cloud mit einem Azure Virtual Network.
5. Vernetzen Sie On-Premises-Geräte mit der Cloud über ein Virtual Private Network (VPN). Eine Leitung mit geringerer Latenz erhalten Sie, wenn Sie ExpressRoute verwenden.
6. On-Premises-Benutzer greifen jetzt ohne Änderungen am Benutzererlebnis auf ihre Anwendungen in der Cloud zu.
7. Die Anwendungen in der Cloud und On-Premises können sicher miteinander kommunizieren und Daten austauschen.

DevOps

Wie schon in Kapitel 8 beschrieben, ermöglicht ein moderner DevOps-Prozess in der Cloud schnelles Veröffentlichen und Iterieren – mehrmals am Tag und manchmal sogar noch öfter. Es kann von Vorteil sein, als Erster ein Produkt auf den Markt zu bringen und ein Marktführer zu werden, anstatt einen Schritt hinter anderen zurückzuliegen.

Die Tools von Microsoft Visual Studio bieten flexible Planung, Quellcodeverwaltung, Paketverwaltung, Entwicklung, Test und automatische Freigabe, um Ihre Anwendung kontinuierlich zu integrieren, testen, liefern und überwachen. Mithilfe von Überwachungstools wie Application Insights sowie Bereitstellungs- und Konfigurationsverwaltungstools wie Chef und Puppet Labs' Puppet können Sie Upgrades so oft wie Sie möchten durchführen.

SharePoint auf Azure

Wenn Sie SharePoint Online noch nicht verwenden, können Sie Ihre Infrastruktur ganz leicht und in wenigen Minuten für Ihre SharePoint-Server erstellen. Sie können Entwicklungs- oder Test-Farmen einrichten oder Ihre SharePoint-Produktionsbereitstellungen horizontal skalieren, indem Sie ihnen sofort weitere Ressourcen hinzufügen. Vereinfachen Sie die Bereitstellung und Konfiguration mit einsatzbereiten Bildern und Vorlagen, die auf erprobten Konfigurationen basieren und reduzieren Sie den Zeitaufwand für die Bereitstellung komplexer SharePoint-Farms von mehreren Tagen auf wenige Minuten. Abbildung A-23 zeigt die Konfiguration.



Abbildung A-23: SharePoint auf Azure

Die nutzungsbasierte Preisgestaltung und die Abrechnung pro Minute von Azure hilft Ihnen, Geld zu sparen. Für Entwicklungs- und Testzwecke können Sie von den Vorteilen von Azure für [Visual Studio-Abonnenten](#) profitieren, um Softwarelizenzkosten zu reduzieren. Beim Testen können Sie je nach Bedarf zusätzliche Server erstellen, um die Skalierung und Auslastung über kurze Zeiträume zu testen und diese zu entfernen, wenn Sie damit fertig sind. Das Verwenden von Ressourcen, die Sie auch tatsächlich benötigen – und nicht mehr – hilft Ihnen dabei, kostengünstiger zu sein.

Dynamics auf Azure

Dynamics 365 ist eine SaaS-Onlinesuite von Unternehmensanwendungen und ermöglicht Geschäftsbasisfunktionen in der Cloud wie ERP, CRM, Lieferkette, Business Intelligence. Dynamics 365 bietet Lösungen für den Vertrieb, Kundendienst, Betrieb, Finanzbereich, Außendienst, Projekt-Service-Automation, Marketing und Erkenntnisse über Kunden.

Die Partner von Dynamics haben ebenfalls viele andere Lösungen entwickelt. Auf [Microsoft AppSource](#) finden Sie Hunderte von Apps, die von Microsoft und unseren Partnern zum Verbessern von Dynamics 365 entwickelt wurden. Suchen Sie Apps nach Name, Branche und Kategorie, laden Sie sie herunter, und beginnen Sie sofort mit der Verwendung. Oder arbeiten Sie mit einem Unternehmen im Microsoft Partner Network zusammen, damit die Apps schnell einsatzbereit sind.

Hybrid Cloud-Szenarien

Beim Erstellen einer hybriden (eine Mischung aus On-Premises und externem Computing) Cloud-Anwendung für Unternehmen oder einer Reihe von Anwendungen entsteht eine Vielzahl an Möglichkeiten zum Vereinfachen der Abläufe und Reduzieren der Kosten. Hier zeigen wir einige Möglichkeiten zur effektiven Nutzung der Cloud für gängige IT-Betriebsszenarien.

Hybrid Cloud-Konnektivität

In der Hybrid Cloud werden einige Anwendungen On-Premises gehosteten, während sich andere in der Cloud befinden. Im Idealfall sollte es für Endbenutzer transparent sein, wo sich diese Anwendungen befinden. Anders gesagt: In der Cloud gehostete Anwendungen sollten im On-Premises-Netzwerk mit der entsprechenden IP-Adresse und -Weiterleitung angezeigt werden. Anwendungen in der Cloud werden über das Azure-Portal so konfiguriert, dass sie sich im selben IP-Bereich wie diejenigen im Rechenzentrum befinden.

Es gibt zahlreiche Ansätze, diese Art der Transparenz des Speicherorts zu erreichen. Die nächsten Abschnitte beschreiben vier separate Möglichkeiten, um ein Rechenzentrum mit Azure zu verknüpfen.

Punkt-zu-Standort

Im Internet können Sie ein solches Virtual Private Network auf zweierlei Arten erstellen. Die erste wird als *Punkt-zu-Standort*-Modell (Abbildung A-24) bezeichnet, bei der das VPN über eine Software auf einzelnen Clientcomputern im Rechenzentrum konfiguriert ist. Punkt-zu-Standort-Verbindungen sind die günstigste Option und sind hilfreich, wenn nur ein paar Computer On-Premises Cloud-Konnektivität benötigen oder wenn die Verbindung von einem Remote- oder Filialbüro ausgeht.

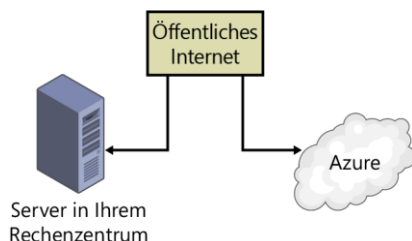


Abbildung A 24: Punkt-zu-Standort-Konnektivität

Standort-zu-Standort

Ein weiterer Ansatz wird als *Standort-zu-Standort*-Konnektivität (Abbildung A-25) bezeichnet. In dieser Konfiguration stellt ein Rechenzentrum einen Hardware-VPN Gateway zur Verknüpfung mit dem gesamten On-Premises-Rechenzentrum mit Anwendungen und Daten in der Cloud bereit. Der Hardwaregateway muss eine öffentliche IP-Adresse aufweisen. Ein Techniker muss verfügbar sein, der die Konfiguration durchführt.

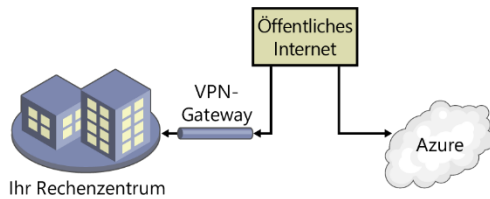


Abbildung A-25: Standort-zu-Standort-Konnektivität

Microsoft Azure ExpressRoute

Viele Kunden wünschen sich eine konfigurierbare und deterministische Netzwerklatenz mit ihrer Cloud-Anwendungen. Sie möchten zudem, dass ihr Netzwerkdatenverkehr vom öffentlichen Internet isoliert wird. Zum Support dieser Anforderungen wird eine Direktverbindung vom Rechenzentrum mit Azure über einen Partner-Telekommunikationsanbieter namens ExpressRoute (Abbildung A-26) bereitgestellt.

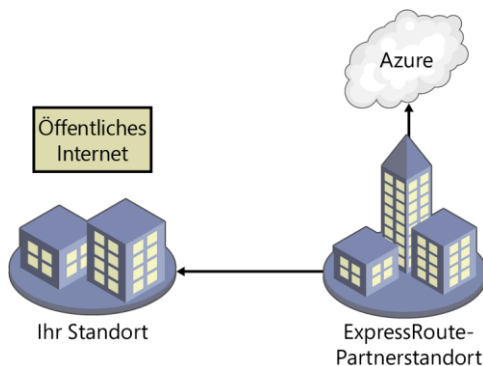


Abbildung A-26: Erstellen einer Verbindung mit dem Rechenzentrum über ExpressRoute

Auch wenn es potenziell eine teurere Lösung ist, bietet ExpressRoute durch eine Verbindung über eine dedizierte Leitung die schnellste Konnektivität sowie eine Isolierung vom Internet.

Eine vollständige Liste der unterstützten Telekommunikationsanbieter für ExpressRoute finden Sie auf der Microsoft-Website.

WAN-Konnektivität

Zudem ist eine Verbindung über einen Telekommunikationsanbieter möglich, sodass Azure einfach als andere Website im WAN-Netzwerk erscheint, wie in Abbildung A-27 dargestellt.

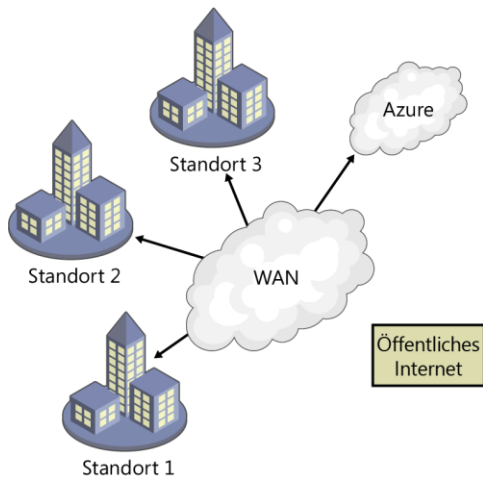


Abbildung A-27: WAN-Konnektivität

Wie beim vorherigen Ansatz können Sie durch das Verwenden eines Telekommunikationsanbieters die Bandbreite mit dem Anbieter verhandeln. Außerdem wird selbstverständlich eine Netzwerkisolierung bereitgestellt. Arbeiten Sie mit Ihrem Telekommunikationsanbieter zusammen, um den besten Ansatz für Ihr Unternehmen zu finden.

In diesen vier Szenarien haben wir Ihnen eine Vielzahl von Ansätzen aufgezeigt, wie Sie Ihre Unternehmens-Rechenzentren mit Anwendungen und Daten in Azure verbinden können. Die Auswahl, die Sie treffen, hängt davon ab, wie Sie den Konflikt zwischen Bandbreite und Kosten berechnen - ob eine Isolierung vom offenen Internet erforderlich ist; und wie Ihre Standorte geografisch verteilt sind.

In den nächsten Abschnitten beschreiben wir eine Reihe gängiger Szenarien auf Anwendungsebene.

Hybrid-Datenbankszenarien

Viele Unternehmen haben erhebliche Investitionen in On-Premises-SQL Server getätigt. Zahlreiche Features erweitern die Funktion des On-Premises-SQL Server auf die Cloud und nutzen die geringen Kosten und enorme Skalierung von Azure.

Beispiel: Sie können eine On-Premises-Instanz von SQL Server mit einer Instanz von SQL Server synchronisieren, die auf einer virtuellen Maschine in Azure (z. B. in einer IaaS-Instanz) oder mit dem Cloud-Nativen SQL Azure ausgeführt wird. Dies ermöglicht beispielsweise verstreuten Teams die Entwicklung auf On-Premises-Instanzen, wie in Abbildung A-28 dargestellt.



Abbildung A-28: On-Premises-SQL Daten in der Cloud veröffentlichen

Zudem können Sie, wie in Abbildung A-29 dargestellt, eine Azure-Instanz von SQL Server als Backup-Ziel für eine On-Premises-Instanz verwenden. Alternativ erhalten Sie eine äußerst kostengünstige Lösung, wenn SQL Server (On-Premises oder Cloud-basiert) im günstigen Azure Blobspeicher gesichert und daraus wiederhergestellt wird.

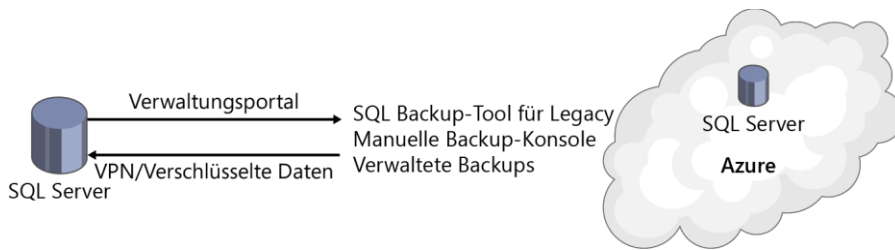


Abbildung A-29: On-Premises-SQL Database Cloud Backup

Letztendlich können Sie als weiteres Muster die Cloud nutzen, um zusätzliche Funktionen für eine On-Premises-Instanz bereitzustellen, wodurch ihre Auslastung reduziert wird. In dem in der Abbildung A-30 dargestellten Beispiel werden zwei Cloud-Replikate angezeigt: eines wird als Backup zur Notfallwiederherstellung aufbewahrt, das andere wird für Business Intelligence (BI)-Anwendungen verwendet.



Abbildung A-30: Verwenden der Cloud-Datenbank als Replikat

Hohe Verfügbarkeit in der Cloud

Viele geschäftskritische Anwendungen erfordern die höchstmögliche Verfügbarkeit und müssen Hardware- und Netzausfällen widerstehen. Das Hosten von Anwendungen in der Cloud bietet zahlreiche Funktionen, einschließlich Redundanz, Fehlertoleranz, widerstandsfähiges Design, die eine hohe Verfügbarkeit ermöglichen.

Denken Sie zuerst über Azure Service Level Agreements (SLAs) nach.¹⁶ Der Azure Compute-Dienst (Anwendungsdienste) bietet beispielsweise eine SLA mit 99,95 %. Eine SQL Database bietet eine SLA mit 99,9 % und Azure Speicher eine SLA mit 99,90 %. Ohne zusätzliche Arbeiten werden Ihrer Anwendung standardmäßig höchstens 108 Minuten Ausfallzeit pro Monat garantiert (von 43.200 Minuten).

Sie können jedoch einiges unternehmen, um diese herausragenden Zahlen zu verbessern. Programmiertechniken wie haltbare Warteschlangen und asynchrone Kommunikation sorgen dafür, dass Anwendungen weniger eng aneinander gekoppelt sind, was die Chancen erhöht, dass ein Ausfall nicht gleich weitere Ausfälle nach sich zieht.

Mit Azure-Verfügbarkeitssätzen wird gewährleistet, dass verschiedene Instanzen von virtuellen Maschinen und/oder verschiedenen Workloads physisch in verschiedenen Racks (andere Stromversorgung, anderer Switch und Server) in einem Azure-Rechenzentrum platziert werden. Verfügbarkeitssätze gewährleisten, dass im Fall eines geplanten oder nicht geplanten Wartungsereignisses oder -fehlers mindestens eine virtuelle Maschine Instanz zur Nutzung verfügbar ist.

¹⁶ Lesen Sie <https://msdn.microsoft.com/de-de/library/azure/dn251004.aspx> für weitere Details.

Sie sind zudem effizient dabei, Anwendungen in Verfügbarkeitsätze einzustufen. Wenn Sie alle Anwendungen der Webebene in einem einzelnen Verfügbarkeitsatz positionieren, wird es unkompliziert, die gesamte Ebene auf einmal neu zu starten oder zu upgraden, da die zugrundeliegende Logik des Verfügbarkeitsatzes gewährleistet, dass mindestens eine der jeweiligen Anwendungen verfügbar ist.

In Abbildung A-31 wird eine Workload auf drei Ebenen verteilt. Jeder Ebene ist ein anderer Verfügbarkeitsatz zugeordnet.

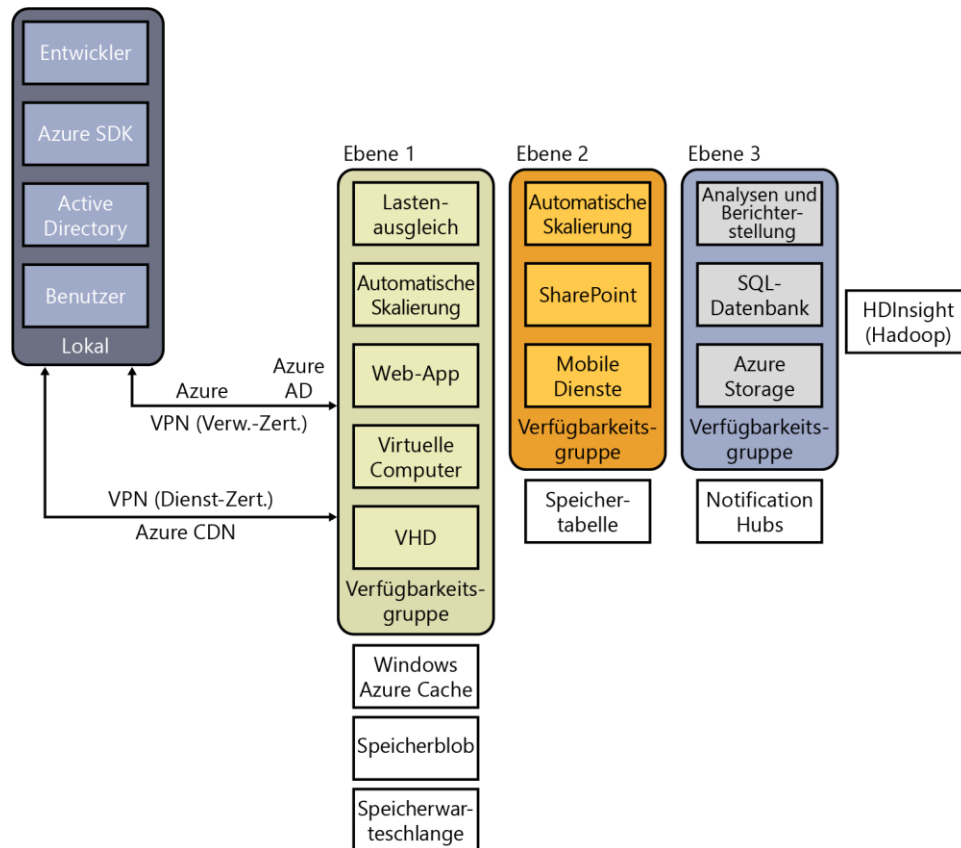


Abbildung A-31: Hohe Verfügbarkeit

Zudem können Sie, wie Abbildung A-32 zeigt, Workloads in geografisch getrennten Rechenzentren platzieren. Sie können Azure Traffic Manager verwenden, um die Abläufe vom primären Rechenzentrum auf das Backup umzustellen, falls ein schwerwiegender Fehler im primären Rechenzentrum auftritt.

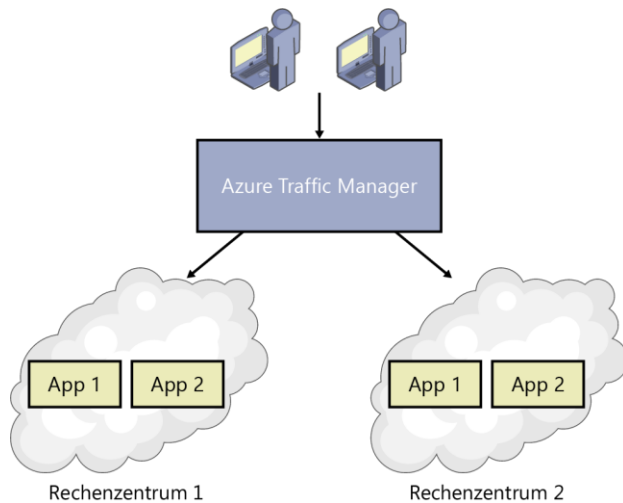


Abbildung A-32: Verwenden verschiedener Geografien

Gestaltungsüberlegungen

Wenn Sie über die Verfügbarkeit Ihrer Anwendungen oder Workloads nachdenken, beachten Sie Folgendes:

- Benötigen Sie eine SLA mit einer Verfügbarkeit von mehr als 99,5 %, dem Standard der Azure SLA?
- Wie viele Instanzen jeder Anwendungs-VM benötigen Sie?
- Welche Anwendungen können asynchrone und lose gekoppelte Programmierungstechniken verwenden, um ihre Verfügbarkeit zu verbessern?
- Würden geografisch redundante Rechenzentren Ihre Workload-Verfügbarkeit im Rahmen Ihrer Kostenparameter verbessern?

Vernetzte Geräte

Das Internet der Dinge verspricht vieles in der Cloud, wie bereits im Buch besprochen, es birgt allerdings auch hohe Anforderungen. IoT-Geräte reichen von medizinischen Sensoren über Fertigungsanlagen, vernetzte Fahrzeuge und Flugzeuge bis hin zur Entwicklung von Umgebungssensoren usw. Prognosen besagen, dass in ein paar Jahren derartige Dinge im zweistelligen Milliardenbereich in beliebiger Form mit dem Internet verbunden sind. In diesem Szenario ist die Cloud für den Empfang, die Analyse und Aktionen an den von IoT-Geräten gesendeten Daten verantwortlich.

Azure bietet zahlreiche Dienste, die das Internet der Dinge ermöglichen. Mit dem Azure Event IoT Hub (Abbildung A-33) können Unternehmen eine Geräteregistrierung erstellen, in der alle zulässigen vernetzten Geräte aufgeführt sind, und können diese verwalten, konfigurieren und bereitstellen. Der IoT Hub von Azure ermöglicht Cloud-Anwendungen, sehr viele Ereignisse (ggf. Milliarden pro Tag) von vernetzten Geräten zu verarbeiten. Azure Stream Analytics kann dann diese Ereignisse in Echtzeit analysieren, Filtervorgänge durchführen und nur die interessanten Ereignisse weiterleiten (wie etwa einen Geräteausfall).

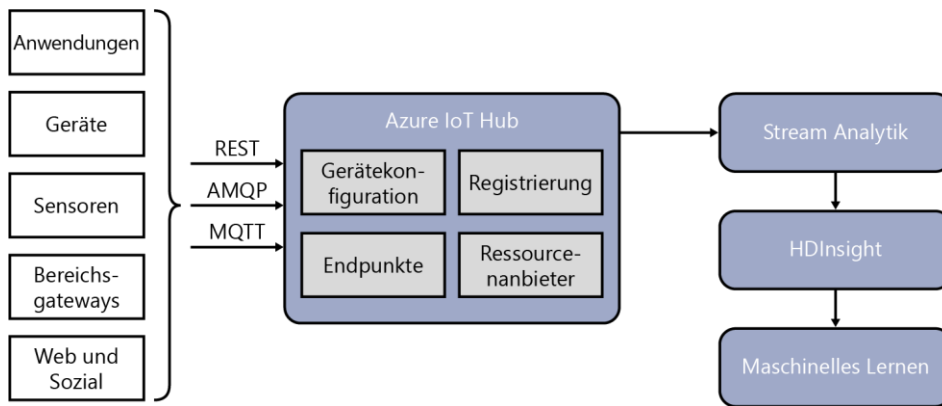


Abbildung A-33: Azure IoT

Zu den weiteren hilfreichen Diensten gehört Azure HDInsight, mit dem große Datenmengen erfasst und Batch analytics programme (z. B. MapReduce) ausgeführt werden können, um Muster zu finden. Azure Machine Learning, die Machine-Learning-Fähigkeit von Azure, kann trainiert werden, um Anomalien zu erkennen und künftige Ausfälle oder Ausfallzeiten vorherzusagen.

Da all diese Geräte mit Ihrer Anwendung vernetzt sind, muss Sicherheit selbstverständlich einen Teil der Architektur ausmachen. Viele IoT-Geräte haben nicht die Rechenleistung, um eine vollständige Verschlüsselung mit öffentlichem Schlüssel oder eine digitale Signatur durchzuführen. Daher sollten Sie mit freigegebenen Zugriffssignaturen (Shared Access Signatures, SAS) vertraut sein und diese möglichst verwenden. Bei einer SAS geht es, wie der Name vermuten lässt, um den *Zugriff*. Das Token enthält in seinen Abfrageparametern die angeforderte URL, eine Ablaufzeit, Berechtigungen und andere Schlüsseldaten. SAS-Token stellen eine effiziente Möglichkeit dar, um sich vor nicht autorisiertem Zugriff durch Eindringlinge auf Ihre Anwendung zu schützen.¹⁷

Gestaltungsüberlegungen

Betrachten Sie beim Gestalten einer Anwendung, die mit dem Internet vernetzte Dinge verwendet, Folgendes:

- Wie viele Geräte vernetzen Sie? Wie häufig werden sie Daten senden und wie groß sind die Nachrichten? Dies hilft Ihnen bei der Bestimmung der Skalierung der Azure Event Hubs, die Sie benötigen, um die Nachrichten zu empfangen und zu verarbeiten.
- Welches Protokoll wird für die Verbindung verwendet (HTTP/REST, AMQP, MQTT)?
- Welche Arten von Daten werden sie senden, und welche dieser Daten sind für Anwendungen hilfreich?
- Müssen die Daten aus einem beliebigen Grund aufbewahrt werden?
- Wie möchten Sie den Status Ihrer Geräte visualisieren? Benötigen Sie ein „Dashboard“ (wie Azure Power BI) zum Sammeln und Visualisieren der eingehenden Daten?

¹⁷ Weitere Informationen über Shared Access Signatures finden Sie unter <https://azure.microsoft.com/documentation/articles/storage-dotnet-shared-access-signature-part-1/> und <https://azure.microsoft.com/documentation/articles/storage-dotnet-shared-access-signature-part-2/>. Es ist wichtig zu erkennen, dass SAS keine ausschließliche IoT-Technologie ist. Sie können sie auch beispielsweise mit Azure Speicher zur Bereitstellung eines delegierten Zugriffs auf Daten verwenden.

Identität und Authentifizierung

Identitätsverwaltung ist der Kern der Sicherheit in der Cloud. Die Identität eines Benutzers bestimmt, auf welche Ressourcen er Zugriff hat. Das Identitätsverwaltungssystem verhindert bei Bedarf nicht autorisierten Zugriff und schützt so die Unternehmensressourcen.

In Azure wird die Identitätsverwaltung von Azure Active Directory (Azure AD) abgewickelt, das auf der Active Directory-Produktfamilie (Branchenstandard) basiert. Azure Active Directory kann zur Authentifizierung von Benutzern bei Cloud-Anwendungen sowie zur Synchronisierung und Erstellung eines Verbunds mit einem On-Premises-Active Directory verwendet werden, damit Benutzer Single Sign-On (SSO) für den Zugriff auf On-Premises- und Cloud-Anwendungen nutzen können.

Mit dem OAuth/OpenID-Protokoll können Sie optional andere Formen der Identität bei Azure Active Directory konfigurieren (Abbildung A-34). Azure AD unterstützt Konten bei Facebook, Google, Yahoo und Microsoft als Identitätsanbieter. Jedem einzelnen können verschiedene Zugriffsebenen gewährt werden. Zudem können Sie vielerlei SaaS-Anwendungen (wie etwa Salesforce.com und viele andere) in Azure AD integrieren. Die mehrstufige Authentifizierung gewährleistet darüber hinaus die Einhaltung von NIST 800-63 Level 3, HIPAA, PCI DSS und anderer gesetzlicher Bestimmungen.

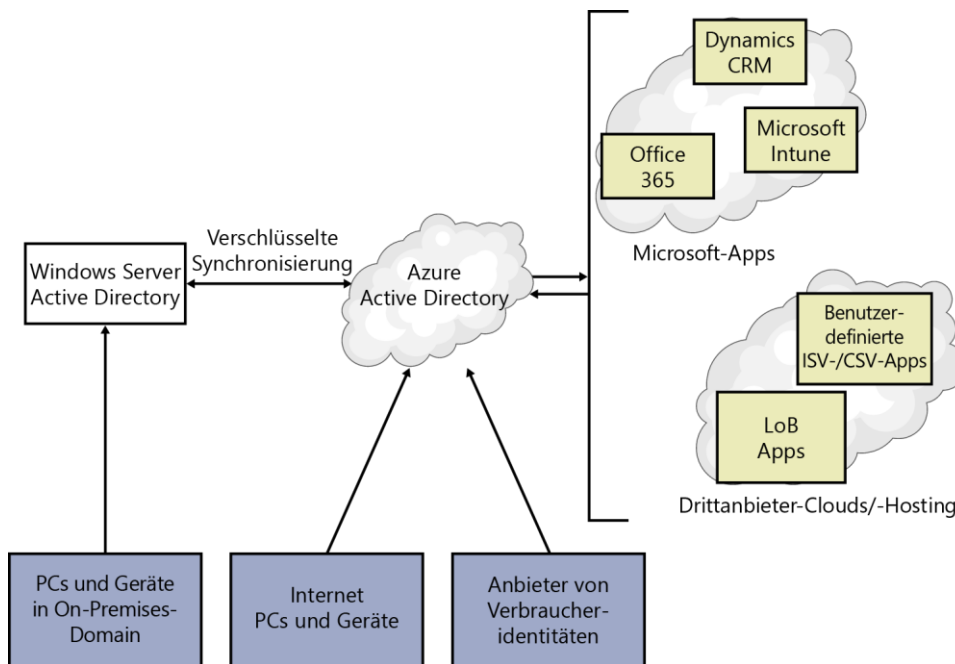


Abbildung A-34: Azure AD-Authentifizierung

Azure Active Directory unterstützt schließlich die zweistufige Authentifizierung (Abbildung A-35) und gewährleistet so eine strikte Identitätsverwaltung. In der Regel authentifiziert sich ein Benutzer zuerst anhand herkömmlicher Anmeldeinformationen wie Benutzername/Kennwort und verwendet dann ein physisches Gerät wie ein Smartphone oder eine Smartcard zum Abschließen des Authentifizierungsprozesses. Azure Active Directory kann ebenfalls so konfiguriert werden, dass ein Smartphone angerufen und eine PIN angefordert wird oder dass angefordert wird, dass ein Badge gelesen werden soll, oder dass eine biometrische Authentifizierung angefordert wird (Beispiel: Fingerabdruck).

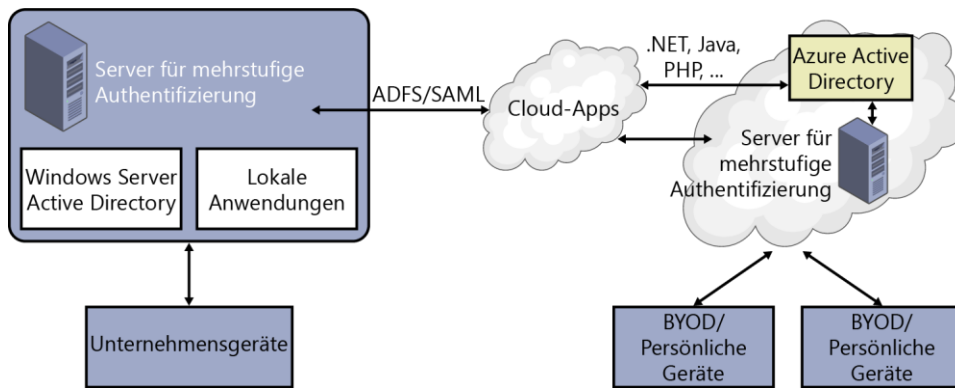


Abbildung A-35: Azure AD Multi-Factor Authentication

Gestaltungsüberlegungen

Es wird behauptet, dass die Identitätsverwaltung der Kern der Cloud ist, da damit der Zugriff auf die Server- und Datenressourcen in der Cloud gesteuert wird. Vor diesem Hintergrund sollten Sie Folgendes beachten:

- Verbinden Ihres On-Premises Active Directory mit Azure AD, um SSO für Cloud-Anwendungen zu aktivieren
- Konfigurieren der Kundenauthentifizierungsmechanismen für bestimmte Typen des Zugriffs (wie etwa E-Commerce-Kunden) auf Ihre Cloud-Anwendungen
- Zweistufige Authentifizierung und damit die strengsten Authentifizierungsanforderungen.

Enterprise Mobility-Verwaltung

2014 wurden eine Reihe mobilitätsbezogener Dienste in ein Paket gepackt, um ein umfassendes Mobilitätsangebot für die IT-Abteilungen von Unternehmen bereitzustellen. Dieses Paket wird als Enterprise Mobility Suite (Abbildung A-36) bezeichnet und umfasst Azure AD und weitere Dienste, wie etwa die Funktion zur Gruppenverwaltung und Self-Service-Kennwortzurücksetzung. Es bietet auch die vorkonfigurierte Anmeldung für zahlreiche SaaS-Anwendungen und Sicherheitsberichterstellung (z. B. für wiederholte Fehler, anomale Anmeldeuster) und kann die zweistufige Authentifizierung unterstützen.

Die Enterprise Mobility Suite beinhaltet zudem ein umfassendes Angebot zur Verwaltung mobiler Geräte (Mobile Device Management; MDM) mit Windows Intune. Dies ermöglicht den IT-Experten die Verwaltung des mobilen Zugriffs auf Unternehmensressourcen sowie die Bereitstellung von Funktionen zur Durchführung der E-Mail-Profilverwaltung, selektives Löschen, Remotesperre und Kennwortzurücksetzung.

Die Enterprise Mobility Suite bietet letztendlich auch Microsoft Azure Rights Management und damit einen zuverlässigen Schutz von Dokumenten für Microsoft Office 365 (Cloud) und On-Premises-Daten.

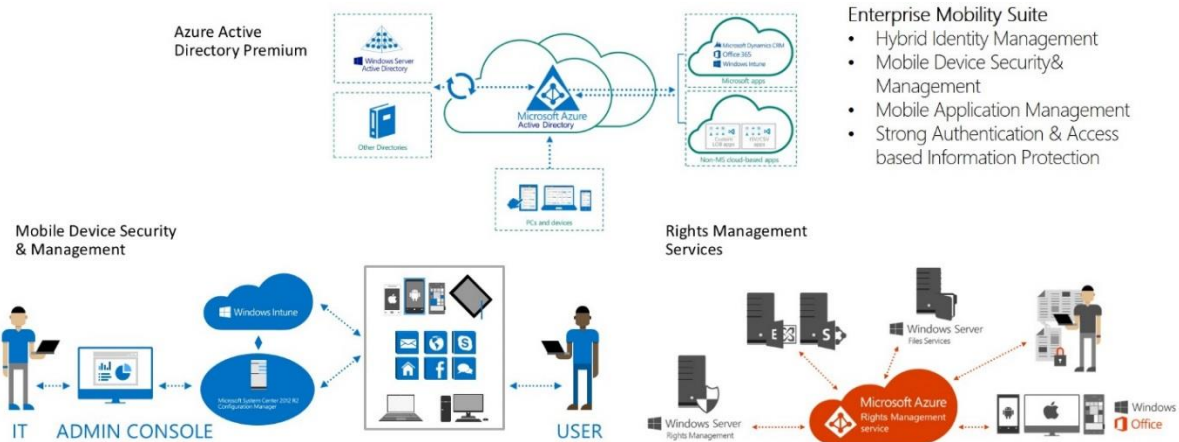


Abbildung A-36: Enterprise Mobility Suite

Gestaltungsüberlegungen

Denken Sie über den Nutzen der Enterprise Mobility Suite nach, wenn eine der folgenden Bedingungen auf Sie zutrifft:

- Sie müssen eine Vielzahl von mobilen Geräten verwalten;
- Sie möchten Benutzern ermöglichen, ihre Kennwörter selbst festzulegen und zurückzusetzen (und dadurch die Belastung für Ihren Helpdesk reduzieren);
- Eine erhebliche Anzahl von mobilen Geräten, die mit Unternehmensnetzwerken vernetzt sind, befinden sich im Besitz der Mitarbeiter. Beispiel: eine „Bring Your Own Device“ (BYOD)-Richtlinie.
- Sie müssen spezifische Datenzugriffsrechte und -richtlinien für verschiedene Benutzer oder Benutzerklassen durchsetzen.

Websites

Mit Azure Web Apps und App Service sind das Erstellen und Pflegen einer komplexen Unternehmenswebsite unkompliziert und günstig. Sie können fortschrittliche HTML5-basierte Websites in jeder verfügbaren Programmiersprache für Webanwendungen entwickeln (.NET, Java, PHP, Node.js und Python). Durch die Vielzahl an Tools kann Ihre Website mit anderen Webressourcen (wie Twitter) und On-Premises-Datenressourcen vernetzt werden. Entwickler können sichere, authentifizierte Webanwendungen mit Active Directory-Features wie Active Directory Authentication Library (ADAL) und der Active Directory Graph-API erstellen. Sie können den Zugriff auf Dokumente über den Rights Management Service von Azure schützen. Wie bereits erwähnt, können Sie eine Verbindung mit Azure AD herstellen und mit einer On-Premises Bereitstellung von Active Directory synchronisieren.

Abbildung A-37 zeigt die Websiteentwicklung, den Zugriff und On-Premises-Ressourcen.

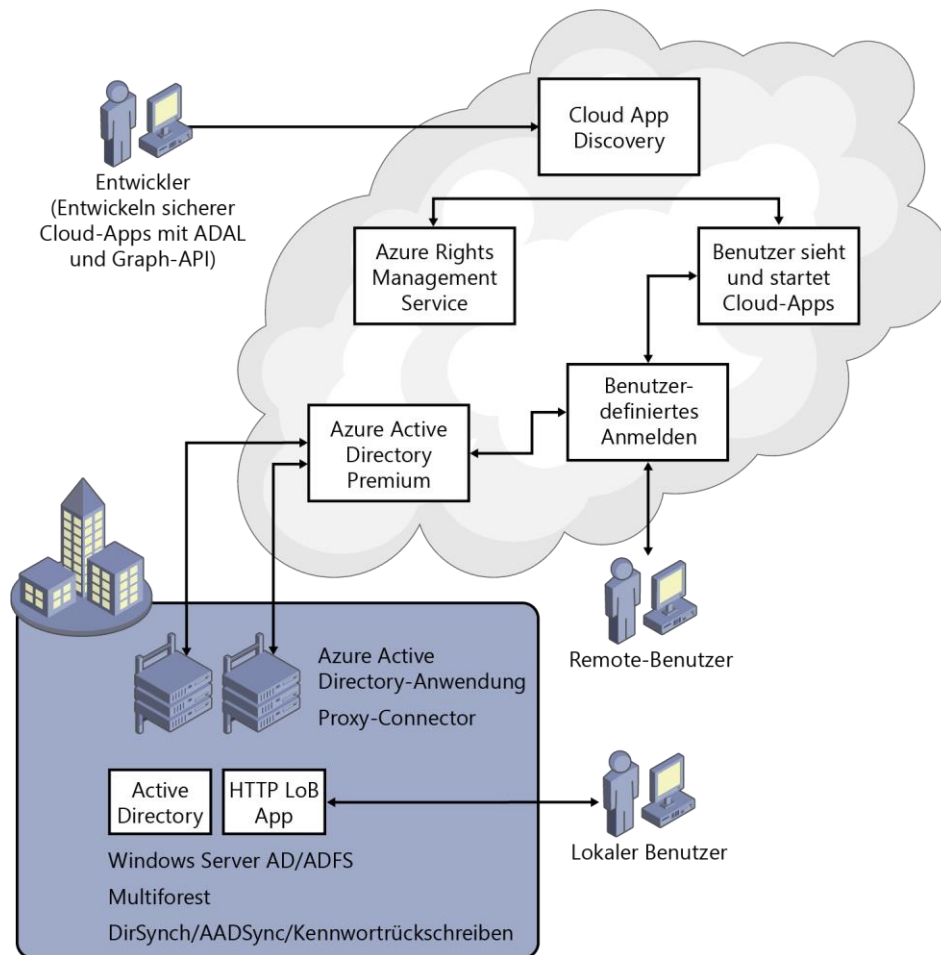


Abbildung A-37: Azure Websites

Gestaltungsüberlegungen

Natürlich entstehen bei der Entwicklung und Bereitstellung einer Website unzählige Gestaltungsprobleme. Hier sind einige, die Sie berücksichtigen sollten:

- Handelt es sich nur um eine Intranetwebsite oder um eine Internetwebsite?
- Wie gehen Sie beim Content Management zur Aktualisierung von Daten vor?
- Muss die Website Benutzer authentifizieren? Falls ja, können sich Benutzer mit externen Anmeldeinformationen wie Konten bei Facebook, Google oder Microsoft authentifizieren? Falls ja, haben sie andere Zugriffsrechte als Unternehmensbenutzer? Azure AD kann eine einfache, umfassende Authentifizierungslösung bereitstellen.
- Welche Arten der Anwendungsintegration in Unternehmensanwendungen benötigen Sie? Sie können BizTalk Server oder Logik-Apps verwenden, um Verbindungen zu On-Premises-Anwendungen wie ERP oder Datenbanken herzustellen.
- Müssen Sie B2B-Transaktionen in Ihrer Datenbank durchführen? Azure BizTalk Services bieten die Möglichkeit, eine Verbindung mit EDI X.12-Anwendungen überall im Internet herzustellen.

Weiterführende Literatur

Azure-Ressourcen

Microsoft-Website <https://www.microsoft.com>

Microsoft Azure Website <https://www.azure.com>

Microsoft Azure Website für Lösungen <https://azure.microsoft.com/solutions/>

Azure Trust Center <https://azure.microsoft.com/support/trust-center/>

Cloud-Technologie [http://download.microsoft.com/download/6/E/4/6E4CB3D1-5004-4024-8D90-6C66C83C17AA/The Economics of the Cloud White Paper.pdf](http://download.microsoft.com/download/6/E/4/6E4CB3D1-5004-4024-8D90-6C66C83C17AA/The_Economics_of_the_Cloud_White_Paper.pdf)

Microsoft Cloud-Rechenzentren <https://www.microsoft.com/cloud-platform/global-datacenters>

Das Whitepaper von Forrester „The Total Economic Impact of Microsoft Azure PaaS“
<https://azure.microsoft.com/resources/total-economic-impact-of-microsoft-azure-paas/>

In Kapitel 1 aufgeführte Fallstudien:

- <https://customers.microsoft.com/story/rollsroycestory>
- <https://customers.microsoft.com/story/brainshark>
- <https://customers.microsoft.com/story/geico>
- <https://customers.microsoft.com/story/accuweather>

Azure Anwendungsarchitektur: Anleitung <https://docs.microsoft.com/azure/architecture/guide/>

Robuste Anwendungen mit Azure entwickeln <https://docs.microsoft.com/azure/architecture/resiliency/>

Resilienz-Checkliste <https://docs.microsoft.com/azure/architecture/checklist/resiliency>

HIPAA:

[http://smb.blob.core.windows.net/smbproduction/Content/Microsoft Cloud Healthcare HIPAA Security Privacy.pdf](http://smb.blob.core.windows.net/smbproduction/Content/Microsoft%20Cloud%20Healthcare%20HIPAA%20Security%20Privacy.pdf)

Einhaltung der Datenschutz-Grundverordnungsrichtlinien

<https://blogs.microsoft.com/blog/2017/05/24/accelerate-gdpr-compliance-microsoft-cloud/>

Cloud-Optimierung:

- <https://www.microsoft.com/itshowcase/blog/determination-sets-8-year-old-on-path-to-save-microsoft-millions-of-dollars/>
- <https://www.microsoft.com/itshowcase/Article/Content/861/Optimizing-resource-efficiency-in-Microsoft-Azure>
- <https://www.microsoft.com/itshowcase/Article/Video/688/Managing-and-optimizing-resources-for-cloud-computing-at-Microsoft> (Webinar)

Externe Websites

Martin Fowlers Blogbeitrag über Microservices <https://martinfowler.com/articles/microservices.html>

Forbes Blogbeitrag über Big Data <https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/>

„Die drei Vs“ von Big Data: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>

Bücher

Jeanne W. Ross, Peter Weill und David C. Robertson *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution*, Harvard Business Review Press, 2006

Gene Kim, Jez Humble, Patrick Debois und John Willis *The DevOps Handbook: How to Create World-Class Agility, Reliability and Security in Technology Organizations*, IT Revolution Press, 2016

Die Autoren



Barry Briggs ist ein unabhängiger Berater mit einer langen Historie in Software- und Enterprise-Computing. Er fungierte in seiner 12-jährigen Laufbahn bei Microsoft in mehreren Rollen. Zuletzt war er als Chief Enterprise Architect im Microsoft DX (Developer Experience)-Team tätig. Die Aufgabe des DX-Teams ist die Gestaltung und Entwicklung epischer Anwendungen mit Microsoft-Kunden, die neue Funktionen der Microsoft-Palette erkunden, einschließlich Microsoft und Open-Source-Produkten und -Frameworks.

Zuvor fungierte Barry Briggs als Chief Architect und CTO für die IT-Organisation von Microsoft. Vorherrschend unter seinen Aufgaben waren der Aufbau und die Leitung des Cloud-Strategie-Teams der Microsoft IT, das für die Strategie und Prozesse hinter der Migration der internen IT-Umgebung von Microsoft in die Cloud verantwortlich war. Zudem leitete er die Enterprise Architecture-Maßnahme, die die Unternehmensstrategien und technologischen Ressourcen auf maximalen Erfolg und Flexibilität ausrichtete. Er leitete eine strategische Inkubationsabteilung, die bahnbrechende Software mit Auswirkungen auf die gesamte IT und Strategien zum Einsatz von Technologien entwickelt, die die tiefe Beziehung der Microsoft IT mit ihren Produktgruppen fördern. Vor der CTO-Rolle leitete Barry Briggs das Team, das die größte Master Data Management (MDM)-Lösung der Welt für Microsoft erstellt hat. Er trat Microsoft 2003 als Senior Architect für Business Process and Integration Division bei, die Microsoft BizTalk Server erstellt hat.

Vor Microsoft fungierte Briggs als CTO für zahlreiche Unternehmen (Aptsoft, Wheelhouse, BroadVision und Interleaf). Davor verbrachte er 11 Jahre bei Lotus/IBM. Dort war Barry viele Jahre lang leitender Architekt für das bekannte Tabellenkalkulationsprodukt von Lotus 1-2-3. Zudem half er bei der Entwicklung von Lotus Notes und leitete die Technologieintegration von Lotus bei IBM nach der Übernahme ein. Er erstellte und leitete zudem das Team, das für die weltweit erste Java-basierte Produktivitätssuite verantwortlich war, Lotus eSuite. 1995 wurde er zum Lotus Fellow ernannt.

Auf seiner Website können Sie sehen, was Barry Briggs gerade vor hat: <http://www.barrybriggs.com>.



Eduardo Kassner ist der Chief Technologie and Innovation Officer bei der „Worldwide Channels & Programs Group“ bei Microsoft Corporation. Sein Team ist für die Definition der Strategie und die Entwicklung der Programme verantwortlich, die die technischen Kapazitäten, praktische Entwicklung und Rentabilität für Hunderttausende von Microsoft Partnern weltweit fördern. Er weist mehr als 26 Jahre Erfahrung in der Verwaltung und Gestaltung komplexer IT-Umgebungen und der Vernetzung der IT und von Geschäftszielen in der Praxis auf. Die von ihm geführten Teams haben dazu beigetragen,

internationalen Konzernen und Regierungen bei diesen Herausforderungen in einem direkten und vernünftigen Ansätzen durch eine Kombination aus strukturierter Framework zu helfen. Er erreicht dies durch Gestalten und Bereitstellen strukturierter Frameworks mit hart verdienter Erfahrung, die die erforderlichen Technologien von Microsoft mit den Rahmen des Geschäftswerts verbindet und die erforderlichen Technologien von Microsoft mit Gleichungen mit schlechten und hervorragenden Amortisationszeiten für Unternehmens- und Behördenumgebungen verknüpfen. Er hat vor kurzem die erste Edition der von Microsoft Press veröffentlichten *Enterprise Cloud Strategy* mitverfasst und veröffentlicht, die mehr als 250.000 Mal von der Azure.com-Website heruntergeladen wurde. Eduardo hat die Teams geleitet, die die Microsoft Cloud-Architekturrolle und weltweite Gemeinschaft sowie Cloud-Nutzungsframeworks, Operations Management, Automation und Architekturmuster gestaltet, eingestellt und verwaltet haben. Er hält regelmäßig Vorträge bei Konferenzen weltweit zu den Themen digitale Transformation, Umstieg in die Cloud und Strategie, Cloud Architektur Best Practices, Öffentliche/Hybrid/Private Cloud, betriebliche Effizienz, IT-ROI und TCO sowie die gesamte Microsoft-Plattform.