

Universität Hamburg  
Fachbereich Informatik

**Microservices und die Zukunft von DevOps**

am Arbeitsbereich Softwarearchitektur (SWA)

Bennet Brunsen, Mathias Schmialek

24. Januar 2016

Blubb

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>4</b>
1.1	Developer . . . . .	4
1.2	Operation . . . . .	4
1.3	Agile Softwareentwicklung . . . . .	5
1.4	Monolith . . . . .	5
<b>2</b>	<b>DevOps</b>	<b>7</b>
2.1	Motivation . . . . .	7
2.2	Maßnahmen . . . . .	7
2.3	Ziele . . . . .	8
<b>3</b>	<b>Microservices</b>	<b>9</b>
3.1	Motivation . . . . .	9
3.2	Architektur . . . . .	9
3.3	Design Entscheidung . . . . .	10
3.3.1	Koordinationsmodell . . . . .	10
3.3.2	Ressourcenmanagement . . . . .	11
3.3.3	Abbildung von architektonischen Elementen . . . . .	11
3.4	Herausforderungen . . . . .	12
3.4.1	Systemstabilität . . . . .	12
3.4.2	Modifizierbarkeit . . . . .	12
3.5	Antipattern . . . . .	13
3.6	Gefahren . . . . .	13
3.7	Beispiel . . . . .	14
<b>4</b>	<b>Zukunft von DevOps</b>	<b>15</b>
4.1	Organisatorische Probleme . . . . .	15
4.1.1	Stackholder mit Einfluss auf Dev und Ops . . . . .	15
4.1.2	Verantwortung und Reorganisation . . . . .	16
4.2	Prozess Probleme . . . . .	16
4.3	Technologische Probleme . . . . .	17
<b>5</b>	<b>Fazit</b>	<b>18</b>

# 1 Einleitung

Lorem Ipsum...

## 1.1 Developer

Viele Betriebe wie zum Beispiel Versicherungen sind heutzutage beinahe vollständig auf Software angewiesen, die ihre Arbeit korrekt abbildet und vereinfacht. Diese Software wird von Entwicklern (Developern) mit Hilfe von Abstraktion und Programmiersprachen hergestellt. Damit die Software auch den Ansprüchen der Anwender entspricht, nimmt der Entwickler die Anforderungen vom Anwender beziehungsweise dem Auftraggeber entgegen und setzt diese in Programmcode um. Zusätzlich ist es die Aufgabe des Entwicklers den geschriebenen Programmcode sowohl manuell als auch programmatisch zu testen und damit ein korrektes Verhalten der Anwendung sicherzustellen.

Das Ergebnis der Arbeit eines Entwicklers ist ein Stück Software, das dem Kunden als Installationsdatei oder Ähnlichem übergeben wird. Der Entwickler selbst ist nicht dafür zuständig, dass die Anwendung in den laufenden Betrieb des Kunden integriert wird.

## 1.2 Operation

Unter Operations werden im herkömmlichen Sinne Mitarbeiter mit IT-Kenntnissen verstanden, deren Ziel es ist, den täglichen IT-Betrieb am laufen zu halten. Zu ihren Aufgaben gehören unter anderem die Bereitstellung von Hardware für Mitarbeiter des Betriebes sowie die Verwaltung von Servern. Sie sind ebenfalls dafür zuständig, Software unter anderem auf die Geräte der Mitarbeiter und auf die Server des Betriebes zu spielen. Dabei kann die Software entweder käuflich erworben oder im eigenen Unternehmen entwickelt worden sein. Dies wird in der Regel mit Skripten realisiert, die Operations selber anlegen.

Zu einer Software, die kommerziell erworben wurde, gibt es in der Regel so genannte Service Level Agreements, die eine mit dem Softwarehersteller vereinbarte Leistungsqualität der einzusetzenden Software beschreiben. Ein Beispiel hierfür wäre, dass ein Hersteller von einer Cloudbasierten Anwendung seinem Kunden verspricht, dass die Anwendung mit einer bestimmten Anzahl an Anfragen innerhalb einer definierten Zeitspanne zurecht kommt, sodass keine Ausfälle entstehen. Innerhalb eines Betriebes überwachen Operations die Service Level Agreements und melden gegebenenfalls Verstöße ihren Vorgesetzten oder dem Hersteller der Software.

Um die Einhaltung der Service Level Agreements zu überprüfen, wird die Software mit Hilfe von Monitoring und Logging Werkzeugen überwacht. Dabei vermitteln die Werkzeuge des Monitorings den Operations wichtige Informationen wie zum Beispiel den Speicherverbrauch und den Status der laufenden Anwendungen. Mit Hilfe der Logging Werkzeuge, können die Operations auf Fehler innerhalb der Anwendung schließen. Für den Fall, dass die Umgebung der Anwendung falsch konfiguriert ist, wird dies üblicherweise in Log-Dateien geschrieben, die

den Operations zur Verfügung stehen.

Wie bereits erwähnt, ist das Ziel von Operations den IT-Betrieb am laufen zu halten. Dies wird in der Regel als Business Continuity bezeichnet. Allerdings ist dies nicht nur mit einer für die Anwendung passend konfigurierten Umgebung möglich. Die Rechner und Server eines Betriebes müssen nach Außen abgesichert werden, um Ausfälle durch Schadangriffe so gut wie möglich zu unterbinden. Dies ist ebenfalls ein Aufgabenbereich von Operations.

### **1.3 Agile Softwareentwicklung**

Neben der klassischen Softwareentwicklung, die nach starren Modellen wie zum Beispiel dem Wasserfallmodell arbeitet, hat sich in den letzten Jahren die agile Softwareentwicklung etabliert. Die agile Softwareentwicklung mit agilen Vorgehensweisen wie zum Beispiel Scrum oder Xtreme Programming, bindet den Kunden stärker in den Entwicklungsprozess ein und bietet die Möglichkeit schon während der Entwicklung auf das die Software Einfluß zu nehmen.

Len Bass hat bei der agilen Softwareentwicklung drei Phasen identifiziert, auf die im folgenden eingegangen wird. Die erste Phase ist die sogenannte Inception Phase. In dieser Phase werden unter anderem die Anforderungen an die Software aufgenommen und erste Modellierungsarbeiten betrieben. Zusätzlich wird in dieser Phase ein Release Plan erstellt, der mit dem Kunden abgestimmt wird.

Die zweite Phase ist die so genannte Construction Phase. In dieser Phase wird die Software nach agilen Methoden wie zum Beispiel Scrum entwickelt. Das Ergebnis dieser Phase ist ein Software Artefakt, das dem Kunden übergeben werden kann.

Die finale Phase ist die Transition Phase. In dieser Phase wird das zuvor hergestellte Artefakt beim Kunden auf die Rechner beziehungsweise Server gespielt und somit in den laufenden Betrieb integriert.

### **1.4 Monolith**

Unter einem Monolithen wird in der Softwareentwicklung ein Architekturstil verstanden, bei dem die Software auf höchster Ebene nur als eine einzelne Komponente gesehen wird. Monolithen sind in der Regel sehr große Komponenten, die mehr als 50.000 Zeilen an Programmcode aufweisen. Darüber hinaus enthalten Monolithen die gesamte Geschäftslogik einer Anwendung. Monolithen entstehen implizit, wenn kein spezieller Architekturstil vorgegeben wird, da die Codebasis mit der Zeit durch weitere Entwicklungsarbeiten wächst. Häufig sind monolithisch entworfene Anwendungen im Serverbereich von Webanwendungen aufzufinden.

Anwendungen, die nach diesem Stil entworfen wurden, weisen einige Nachteile auf. Zum einen erfordert jede Änderung (zum Beispiel eine Fehlerkorrektur) ein erneutes Deployment der gesamten Anwendung. Zusätzlich skalieren monolithische Anwendung schlecht. Sollte zum Beispiel eine logische Einheit des Monolithen wie die Datenpersistierung nicht unter der aktuellen Last bestehen, müsste eine zweite Instanz der gesamten Anwendung erzeugt werden, um die Last zu bewältigen. Dies ist nicht optimal, da eigentlich nur die Datenpersistierung zusätzliche Instanzen benötigen würde.

Ein weiterer Nachteil, der durch die monolithische Architektur entsteht, findet sich im Release einer neuen Version wieder. Da bei einem erneuten Deployment die gesamte Anwendung erneut auf die Rechner beziehungsweise Server gespielt werden muss, sind diese in der Zeit

des Deployments nicht verfügbar. Dies kann je nach Anwendungsfeld zu einem Ausfall an Einnahmen führen. Zum Beispiel könnte ein Händler im Internet keine Produkte verkaufen, während seine Anwendung nicht verfügbar ist. Aus diesem Grund werden neue Versionen einer monolithischen Anwendung so selten wie nötig auf die Systeme gespielt. Dies führt wiederum dazu, dass eine neue Version nicht bei jedem neuen Feature entsteht, sondern erst mit einer Vielzahl neuer Features. Die vielen neuen Features können allerdings Inkompatibilitäten in der Anwendung erzeugen sowie zu einer erhöhten Fehleranfälligkeit führen. Daher erfordert eine neue Version einen sehr hohen Aufwand beim Testen der Anwendung. Darüber hinaus kann eine neue Version auch eine völlig anders konfigurierte Umgebung erfordern, was den Aufwand einer neuen Version ebenfalls erhöht. All dies erfordert einen sehr hohen Koordinationsaufwand und eine langfristige Planung, was wiederum zu einem langsamen Release der Anwendung führt.

## 2 DevOps

Unter dem Begriff DevOps werden eine Menge an Maßnahmen, die die Bereiche Development und Operations enger zusammenführen, verstanden. In diesem Kapitel wird zunächst die Motivation von DevOps beschrieben. Im Anschluss werden einige Maßnahmen, die DevOps ermöglichen vorgestellt. Zum Abschluss des Kapitels werden noch ein mal die Ziele von DevOps hervorgehoben.

### 2.1 Motivation

DevOps bietet einem Softwarehersteller viele Vorteile. Unter anderem wird das Prinzip des Continuous Deployment, das die Zeit zwischen der Entwicklung einer Anwendung und dem Release dieser Anwendung verringert, ermöglicht. Beim Continuous Deployment wird direkt nachdem ein Entwicklerteam neuen Code innerhalb einer Versionsverwaltung wie zum Beispiel Git freigegeben hat, dieser mittels Automatisierung auf die Zielsysteme gespielt. Dadurch ermöglicht Continuous Deployment einem Softwarehersteller neue Features schneller zu veröffentlichen und unter Umständen einen Vorteil gegenüber der Konkurrenz zu erzielen.

Zusätzlich sollte die benötigte Koordination zwischen Development und Operations verringert werden. Des Weiteren ermöglicht DevOps Einsparungen in den benötigten Kapazitäten des Operation Teams. Dies wird mittels Automatisierung gängiger Aufgaben von Operations wie der Analyse von Systemlogs, der Erstellung von Backups, der Optimierung von Systemperformance oder der Lösung von identifizierten Problemen ermöglicht.

### 2.2 Maßnahmen

Wie bereits erwähnt umfasst der Begriff DevOps die Maßnahmen, die Development und Operations näher zusammenführen sollen. Eine dieser Maßnahmen ist die Berücksichtigung von Operations bei der Softwareentwicklung. Da Operations auf Werkzeuge zum Logging und Monitoring einer Anwendung angewiesen sind, sollen Entwickler geeignete Logs und Schnittstellen zum Monitoring innerhalb der Anwendung zur Verfügung stellen. Zusätzlich sollen die Entwickler eine möglichst hohe Anzahl an Informationen für das Incident Handling bereit stellen. Dies kann durch eine hohe Anzahl an beschriebenen Fehlertypen innerhalb der Anwendung realisiert werden.

Zusätzlich fordert DevOps, dass Entwickler für das Behandeln ernsterer Incidents (Vorfälle) verantwortlich gemacht werden. Sollte ein Programm einen Fehler aufweisen, der zum Beispiel nicht trivial durch eine angepasste Umgebungsvariable zu lösen ist, sollen sich die Entwickler des Problems annehmen.

Des Weiteren erfordert DevOps, dass Development und Operations denselben Deployment Prozess verwenden. Das bedeutet, dass Entwickler während der Entwicklung ihren Programmcode mit den selben Werkzeugen beziehungsweise Skripten auf ihre Testumgebung spielen, die Operation in der Transitionphase ebenfalls verwenden würden.

Zusätzlich legt DevOps großen Wert auf eine saubere Infrastruktur. Daher muss laut DevOps auch die Infrastruktur den selben Qualitätsanspruch wie Anwendungscode entsprechen. Dies kann durch Anwendung von Qualitätssicherungs Praktiken erfolgen.

Darüber hinaus ist kontinuierliches Deployment mittels Automatismen wie zum Beispiel Tests oder Build Skripten ein zentraler Bestandteil von DevOps.

## **2.3 Ziele**

DevOps verfolgt mit den bereits genannten Maßnahmen sehr wichtige Ziele. Zum einen sollen die Mitarbeiter innerhalb von Operations durch die Automatismen, die DevOps erfordert entlastet werden und zum anderen soll der Koordinationsaufwand zwischen Operations und Development stark reduziert werden. Zusätzlich soll ein vereinfachtes und weniger Fehleranfälliges Deployment von neuen Versionen einer Software ermöglicht werden.



## 3 Microservices

In diesem Kapitel werden Microservices genauer betrachtet. Dazu wird zunächst der Zusammenhang zwischen DevOps und Microservices erläutert. Es wird gezeigt, dass Microservices optimal geeignet sind die Anforderungen von DevOps zu erfüllen. Daraufhin werden Architektur, Eigenschaften sowie Herausforderungen von Microservices vorgestellt. Dies wird immer unter dem Gesichtspunkt betrachtet, dass Microservices für DevOps eingesetzt wird. Dementsprechend werden stets die Punkte hervorgehoben, die für oder gegen den Einsatz in DevOps sprechen. Zum Schluss dieses Kapitels werden noch einige Gefahren und Antipattern vorgestellt.

### 3.1 Motivation

Entwicklerteams, die die DevOps Praktiken anwenden, sind üblicherweise sehr klein und haben geringe Koordination zu anderen Teams. Dadurch haben die Teams eine begrenzte Übersicht über die gesamte Anwendung. Sobald allerdings neu entwickelte Komponenten eingesetzt werden sollen, ist es zwingend notwendig Kompatibilität zu anderen Komponenten sicher zu stellen. Dies kann zum einen durch teamübergreifende Koordination oder durch den Einsatz einer bestimmten Architektur gelöst werden.

Des weiteren fordern die DevOps Praktiken das continuous Deployment. Dies sollte stets ohne große architektonische Anpassungen einsetzbar sein, um so die benötigte Zeit für die Einführung einer neuen Komponente möglichst gering zu halten. Weitere Anforderungen an die Architektur sind: Unterstützung unterschiedlicher Versionen einer Komponente, sodass Teammitglieder ohne größere Koordination eigene Neuentwicklungen einsetzen können. Ebenso sollen Rollbacks möglich sein, um zum einen live testing zu ermöglichen und im Fall von Fehlern die eingesetzte Komponente zurück zu setzen.

Diese Anforderungen werden allesamt von der Microservice Architektur erfüllt. Im folgenden Abschnitt wird diese Architektur genauer erläutert.

### 3.2 Architektur

Bei der Microservice Architektur besteht die Softwareanwendungen beziehungsweise der Business Services aus mehreren kleinen Komponenten. Diese Komponenten werden Microservices genannt, der eine angeschlossene kleine Funktion der Anwendung beinhaltet. Jede Komponente ist einzeln ausführbar, dies hat den Vorteil, dass für die Bereitstellung eines Microservices keine weiteren Komponenten benötigt werden und so keine beziehungsweise nur geringe Abhängigkeiten bestehen. Dementsprechend verfügen Microservices, sofern sie es benötigen, über ihre eigene Datenbank auf die nur sie zugreifen können.

Die Funktionen und Daten eines Microservices werden über das Interface des Microservices

angeboten. Die Kommunikation zwischen den Microservices verläuft über das Netzwerk. Üblicherweise wird dafür ein simples Kommunikationsprotokoll wie HTTP verwendet. Der Aufruf eines oder mehrerer Microservices von einem Microservice bildet den gesamten Business Service. Abbildung ?? zeigt ein Beispiel.

Instanzen eines Services werden in einer Registry verwaltet und sobald ein Service eine Funktion eines anderen Services benötigt, fragt der Service bei der Registry nach diesem Service und erhält die benötigten Daten. Der genaue Ablauf der verschiedenen Akteure wird im folgenden Abschnitt genauer betrachtet.

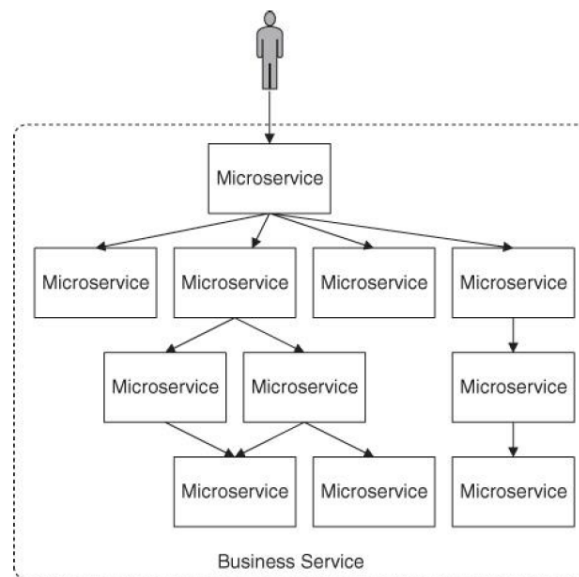


Abbildung 3.1: Business service

### 3.3 Design Entscheidung

In diesem Abschnitt wird zunächst das Koordinationsmodell mit den drei Akteuren *Client*, *Service* und *Registry/Load Balancer* vorgestellt. Daraufhin wird auf das Ressourcenmanagement von Instanzen eingegangen. Dazu werden Szenarien vorgestellt, die die Anzahl der Instanzen eines Microservices regulieren. Zum Schluss wird die Arbeitseinteilung und Zuweisung der architektonischen Elemente (Komponenten) erläutert. Dabei werden Möglichkeiten präsentiert, die die Microservice Architektur anbietet und daraufhin welche dieser Möglichkeiten für DevOps geeignet sind.

#### 3.3.1 Koordinationsmodell

Beim Koordinationsmodell gibt es drei Akteure. Zum einen die *Registry/Load Balancer*, wobei die Registry für die Verwaltung der Serviceinstanzen zuständig ist und der Load Balancer für die Verteilung der Last auf die verschiedenen Instanzen eines Services. So kann beispielsweise der Load Balancer bei erhöhter Anzahl von Anfragen auf einen Service weitere Instanzen anfordern, sodass Instanzen nicht überlastet werden.

Der zweite Akteur ist die *Instanz eines Services*, die Daten beziehungsweise Dienstleistungen anbietet. Die Instanz registriert sich bei der Registry und hinterlegt ihren Namen, Adresse und Interface. Daraufhin steht nun die Instanz für den dritten Akteur bereit: Der *Client* kann dabei ein Benutzer oder ein Service sein, der für einige Aufgaben weitere Services benötigt. Dafür fragt dieser bei der Registry nach den gewünschten Service und erhält die hinterlegten Daten der Serviceinstanz. Mit diesen Daten kann der Client nun die Instanz über das Interface ansprechen und verwenden. Die folgende Abbildung 3.2 gibt eine Übersicht der Beziehungen der drei Akteure.

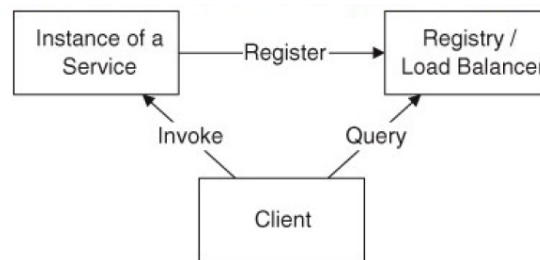


Abbildung 3.2: Die drei Akteure der Microservice Architektur

Da es jederzeit Möglich ist, dass Instanzen ausfallen können oder nicht mehr aktiv sind, ist es wichtig, dass die Registry über diese Instanzen informiert ist. Denn sonst vermittelt die Registry Instanzen an Clienten, die der Client nicht ansprechen kann. Für dieses Problem existiert der Healthcheck. Dabei werden Instanzen nur für eine bestimmte Zeit in der Registry verwaltet. Damit Instanzen nicht aus der Registry entfernt werden, müssen sich die Instanzen periodisch bei der Registry melden. Alternativ kann die Registry proaktive Anfragen an Instanzen stellen, die in der Registry registriert sind. Sollte die Instanz nach bestimmter Zeit keine Antwort liefern wird diese aus der Registry entfernt.

### 3.3.2 Ressourcenmanagement

Ein wichtiger Anforderungspunkt von DevOps ist die Skalierbarkeit. Weitere Serviceinstanzen lassen sich bei Ausfällen von Instanzen oder bei höherer Belastung initialisieren. Auch ist es möglich Instanzen bei geringerer Belastung zu entfernen um so Ressourcen zu sparen. Bei der Entscheidung welcher Akteur über die Anzahl der Instanzen bestimmt gibt es drei Szenarien: Zum einen kann der Service selber entschieden ob er von sich weitere Instanzen bereitstellt, dies geschieht wenn der Service erkennt, dass Instanzen überbelastet sind. Zum Anderen kann der Client weitere Instanzen anfordern, sofern dieser bereits im Vorfeld weiss, dass er in naher Zukunft eine erhöhte Anzahl von Anfragen an einen Service hat. Im dritten Szenario kann eine externe Verwaltung durch Monitoring über die Anzahl der Instanzen entscheiden. So kann durch Monitoring erkannt werden, dass zu bestimmten Uhrzeiten ein Service vermehrt verwendet wird. Beispielsweise am Abend oder Wochenende, wo viele Benutzer zuhause sind und den Service von ihnen verwendet wird.

### 3.3.3 Abbildung von architektonischen Elementen

Bei der Arbeitsaufteilung von Teams, können zum einen mehrere Teams einem Service arbeiten und ein Team an mehreren Services. Dies benötigt allerdings ein erhöhten Koordinationsauf-

wand. Idealerweise arbeiten an einem Service nur ein Team, wobei ein Team für mehreren Services zuständig sein kann. Dies entspricht auch den Anforderungen von DevOps, das geringe Koordination zwischen den Teams fordert.

Neben der Entwicklung einer Komponente von nur einem Team, sollen die Komponenten auch unabhängige Einheiten darstellen. So können diese unabhängig ausgeliefert werden und Änderungen haben keine Auswirkung auf andere Komponenten. Dies verringert ebenfalls die Koordination und beschleunigt die Auslieferung einzelner Komponenten. Die Anforderungen des continuous Deployment des DevOps werden damit ebenfalls erfüllt.

## 3.4 Herausforderungen

Aufgrund der Eigenschaften, wie geringe Koordination zwischen Teams, hat die Architektur einige Herausforderungen. Dazu zählt zum einen die Systemstabilität und leichte Modifizierbarkeit der Module bei Erkennung von Problemen, wie beispielsweise neuen Versionen von benutzter Dritt-Software. Im folgenden werden die Herausforderungen der Microservicearchitektur genauer betrachtet.

### 3.4.1 Systemstabilität

Clients sprechen Service über ein Interface an. Diese Interface können sich im Laufe der Entwicklung verändern. Aufgrund der geringen Koordination zwischen den Teams, können Missverständnisse bezüglich der Semantik der Interface zwischen Client- und Service Team entstehen. So können Service mit neuen Interface einen unerwarteten Input erhalten, oder Clients von einem Service mit neuen Interface ein unerwarteten Output. Um diesen Problemen entgegenzuwirken ist defensives Programmieren gefordert, das heißt es benötigt eine große Anzahl unterschiedlicher Exceptions um die Fehler eingrenzen zu können. Zwar ist es möglich bei neuen Änderungen von Services Integrationstests durchzuführen, dies ist allerdings auf Grund der kurzen Releasephasen und der hohen Anzahl von Microservices sehr mühsam und Zeitaufwendig. Daher wird der *Consumer driven contract* verwendet. Für jeden Microservices werden Testcases erstellt, die den Input und Output festlegen. Sobald die Interfacespezifikationen geändert werden, müssen die Testcases angepasst werden und von den Clients, die den Service verwenden, akzeptiert werden.

Ein weiterer Punkt für die Sicherstellung der Systemstabilität ist die Korrektheit der Umgebung. Systemumgebungen können fehlerhaft oder falsch konfiguriert sein. Damit der Service dennoch einwandfrei läuft muss bei der Initialisierung die Umgebung geprüft werden und gegebenenfalls muss sich der Service der Umgebung anpassen oder der Service passt die Umgebung an.

Ausfälle von Instanzen sind keine Seltenheit. Diese Ausfälle können mit Hilfe von Timeouts ermittelt werden und Clients müssen alternative Mechanismen bei Timeout bereitstellen und ausführen.

### 3.4.2 Modifizierbarkeit

Modifizierbarkeit bedeutet, dass Services leicht und schnell auf Änderungen angepasst werden können. Zwar ist es schwer ein Service so robust zu programmieren, dass auf jedes mögliche

Problem schnell reagiert werden kann. Dennoch sollte der Service schnell die wahrscheinlichsten Änderungen identifizieren. Dazu gehört die Umgebung eines Services, das auf verschiedenen Rechnern unterschiedlich konfiguriert sein kann. Auch kann sich ein Zustand eines anderen verwendeten Services verändern. Das Interface sowie die angebotene Dienstleistung kann auf einer anderen Art bearbeitet werden, die möglicherweise mehr Zeit in Anspruch nimmt.

Neue Versionen von verwendete Bibliotheken und Dritt-Software können ebenfalls veränderte Funktionalität haben und so zu Problemen führen.

Da üblicherweise auf identifizierte Veränderungen nicht direkt reagiert werden kann, wird versucht kaskadierende Effekte so gering wie möglich zu halten, sodass andere Bereiche nicht ebenfalls von den Problemen betroffen werden. Dazu werden mit Hilfe von Modulen die Änderungen gekapselt. Module sind in jeden Service enthalten und lokalisieren sowie isolieren Änderungen. Außerdem bieten die Module ein stabiles Interface zu den Änderungen an, sodass der Service möglichst normal weiterarbeiten kann.

### 3.5 Antipattern

In diesem Abschnitt werden einige Antipattern vorgestellt und gezeigt wie die korrekte Vorgehensweise ist.

Funktionsumfang eines Services wächst mit der Zeit und den Anforderungen:

Services sollten möglichst klein gehalten werden und neu eingeführte Funktionen sollten jeweils einen neuen Service bilden. Zu wenig Automatisierung der Test und des Deployments:

Um kurze Releasephasen einzuhalten ist es wichtig in allen möglichen Bereichen zu automatisieren, da sonst zu viel Zeit verloren geht.

Horizontale Schichten werden als Services abgebildet (z.B. Datenschicht und Geschäftslogik): Microservices sollten möglichst unabhängig und einzeln ausführbar sein. Sobald Datenschicht und Geschäftslogik getrennt wird, benötigt mindestens ein Service für den Zugriff auf die Datenbank immer einen anderen Service. Dies entspricht nicht den gewünschten Eigenschaften von Microservices.

Jeder Service wird manuell konfiguriert:

Muss beispielsweise eine Internetadresse in den Services geändert werden, würde es sehr zeitaufwendig sein die Änderungen in jeden Service einzeln auszuführen. Daher sollten die Services mit einem Konfigurationsserver verbunden sein und Änderungen über diesen Server ausgeführt werden.

Zu jedem Service existiert nur eine Version:

Kurze Releasephasen bedeuten häufige Versionsänderungen. Existiert nur eine Version hat dies zur Folge, dass alle Instanzen der alten Version zerstört werden müssen. Dabei könnten diese Instanzen allerdings gerade von Clients in Benutzung sein. Daher sollten nur Instanzen durch Serviceinstanzen der neuen Version ersetzt werden, wenn sie nicht verwendet werden.

### 3.6 Gefahren

Microservices beinhalten einige Gefahren. Die hohe Anzahl an Netzwerkverbindungen für die Kommunikation zwischen den Services, Clients und der Registry kann zu möglichen Latenzen führen. Wodurch fälschlicherweise Timeouts ermittelt werden können. Auch verschlechtert sich

die Effizienz des Business Services, da Clienten länger auf die Antwort eines Services warten muss.

Unerwartete Überlastungen von Serviceinstanzen verlangsamen die Performance. Ebenso führen Ausfälle von Instanzen zu geringerer Effizienz der gesamten Anwendung.

Bei einer hohen Anzahl von Serviceinstanzen kann es dazu kommen, dass die Registry nicht mit der Verwaltung der Instanzen hinter herkommt und es bei der Vermittlung der Instanzen an die Clienten zu Verzögerungen kommt oder sogar zur falschen Vermittlung einer Instanz.

### **3.7 Beispiel**

Ein Beispiel für den Einsatz von Microservices ist Netflix. Ihr ganzes Streamingsystem ist auf der Microservicearchitektur aufgebaut. Durch die leichte Skalierbarkeit und Updaten von Microservices im laufenden Betrieb erreicht Netflix eine Verfügbarkeitsquote von 99.7%. Im Schnitt ist Netflix nur zwei Stunden im Monat nicht verfügbar.

## 4 Zukunft von DevOps

DevOps ist ein neuer Ansatz und wird aktuell fast nur von den Innovatoren wie Netflix, Amazon und Google angewendet. Enterprise Unternehmen sind ebenfalls an continuous delivery und deployment interessiert und denken über den Einsatz von DevOps nach. Für Startup Unternehmen ist DevOps nicht von Bedeutung, da ihr Fokus auf Kundengewinnung liegt. Erst beim Wachsen des Unternehmens benötigen sie eine flexiblere Architektur, wie die DevOps anbietet.

Aufgrund der geringen Verbreitung sind die Vorteile von DevOps gegenüber der aufwendigen Einführung noch nicht eindeutig abzuschätzen. Erst sobald mehrere Unternehmen DevOps einführen, ist die Kluft überwunden und viele weitere Unternehmen entscheiden sich für die Einführen von DevOps. Abbildung 4.1 zeigt die Entwicklung der Einführung beispielsweise einer neuen Architektur. DevOps ist momentan dabei die Kluft (Chasm) zu überspringen.

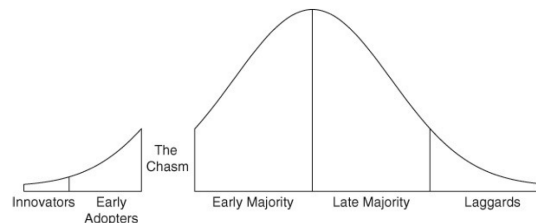


Abbildung 4.1: Chasm

Im folgenden wird auf einige Probleme und Anforderungen eingegangen, die DevOps mit sich bringen.

### 4.1 Organisatorische Probleme

#### 4.1.1 Stackholder mit Einfluss auf Dev und Ops

DevOps versucht Dev und Ops zusammen zu führen um den Koordinationsaufwand zu verringern. Allerdings existieren einige Stakeholder, die Einfluss auf Dev und Ops haben und Probleme verursachen.

Businessverantwortliche haben großen Einfluss in den meisten Bereichen der Organisation. Neue Produkte oder Änderungen in der Versorgungskette haben Auswirkungen auf Dev und Ops. Durch kurze Entwicklungs- und Produktionsphasen bleibt nicht viel Zeit für die Koordination zwischen Businessverantwortlichen, Devs und Ops. Daher regelt der *BizOps* die Koordination zwischen den drei Parteien.

Der Datenanalytiker betreibt mit Hilfe von beispielsweise Clustern Datenanalyse. Der gewonnene Einblick in das Business hilft Kundenverhalten zu verstehen und Bereiche für Optimierung zu finden.

Der Sicherheitsprozess muss agil gehalten werden, um mit dem continuous deployment mitzuhalten. Dies ist nicht nur eine organisatorische Angelegenheit, sondern auch Abhängig der Sicherheitsprüfer.

#### **4.1.2 Verantwortung und Reorganisation**

Microservices werden von kleinen Teams verwaltet, allerdings von vielen anderen Teams aufgerufen. Sobald eine neue Version eines Services ausgeliefert wird, muss nicht nur sichergestellt werden, dass der Service andere Services korrekt benutzen kann, sondern auch dass andere Services den eigenen Service korrekt verwenden können. Eine Lösung dafür ist, dass Teams, die den neuen Service verwenden, bei der test suite Erstellung beteiligt sind. Sie sind also Co-Verantwortliche für den Service.

### **4.2 Prozess Probleme**

Durch die DevOps Praktiken entstehen auch eine Vielzahl an Prozess Problemen. Es wird unter anderem für das Continuous Deployment eine so genannte Continuous Deployment Pipeline benötigt. Eine solche Pipeline besteht aus einer Vielzahl von Werkzeugen und ist dafür gedacht, den Programmcode auf eine Plattform zu deployen. Jedes dieser Werkzeuge kann allerdings eine Abhängigkeit zu dem Hersteller des Werkzeuges zur Folge haben, was die Portierbarkeit der Anwendung erschwert. Eine Möglichkeit solche Abhängigkeiten zu verhindern besteht darin bei dem Deployment auf gängige Standards zu setzen. Derzeit existieren allerdings noch keine akzeptierten Standards für die Werkzeuge innerhalb einer Continuous Deployment Pipeline. Durch eine höhere Verbreitung von DevOps, könnten in naher Zukunft tatsächlich Standards beschlossen werden.

Es existieren dennoch Strategien, um das Problem der Herstellerabhängigkeit zu minimieren. Zum einen sollte bei der Entwicklung auf einen defensiven Entwicklungsstil gepocht werden. Zum anderen existieren für eine Vielzahl von Werkzeugen Migrationswerkzeuge auf andere Werkzeuge. Diese Migrationswerkzeuge funktionieren allerdings nur bedingt gut und der Erfolg einer Migration hängt davon ab, ob nur eine Obermenge an Funktionen beider Werkzeuge verwendet wird.

Ein weiteres Prozess Problem, das durch die DevOps Praktiken entsteht, ist eng mit der Häufigkeit der Deployments verbunden. Eine gut funktionierende Deployment Pipeline ermöglicht häufigere Deployments. Dies bringt eine diverse Herausforderungen mit sich. Zunächst muss die Zeit zum Testen der Anwendung verringert werden. Dies kann zur Folge haben, dass Fehler nicht rechtzeitig entdeckt werden. Daher muss ein Rollback auf eine vorherige Version bei einem Fehler möglich sein. Der Fehler könnte mit dem darauf folgenden Deployment behoben sein. Zusätzlich muss eine automatische Fehlererkennung Bestandteil der Anwendung sein, damit bei Eintreten eines Fehlers automatisch ein Rollback stattfinden kann.

Durch häufigeres Deployment sind Unternehmen in der Lage, in kurzer Zeit viele neue Services anzubieten, was sowohl das Verhalten der Nutzer als auch die Last auf verschiedenen Services verändern kann. Zusätzlich kann auch das Deployment in eine Umgebung fälschlicherweise zu einem Alarm innerhalb eines Monitoring Tools der Umgebung führen.

All dies hat zur Folge, dass Unternehmen, die DevOps einsetzen, die Art ihres Monitorings und ihrer Qualitätssicherung verändern müssen.



### 4.3 Technologische Probleme

In der Regel sind die Werkzeuge einer Continuous Deployment Pipeline durch Skripte zur Integration miteinander verbunden. Um weitere Werkzeuge einzufügen bedarf es einer Änderung dieser Skripte. Dieser Ansatz bringt eine Vielzahl an Problemen mit sich. Es wird durch die Skripte schwerer nachvollziehbar, welche Komponenten auf welche Plattform deployed werden. Zusätzlich enthalten Services in der Regel keine Informationen mit welchen Werkzeugen sie deployed wurden. Daher wird eine Fehleranalyse bei einem korrupten Deployment erschwert. Ein weiteres Problem entsteht dadurch, dass die Werkzeuge häufig die Sicherheitsinformationen wie Nutzernamen und Passwörter von einem Werkzeug zum nächsten weitergeben müssen und dadurch die Sicherheit gefährdet wird.

Das größte Problem besteht allerdings darin, dass viele Werkzeuge an sich nicht für Continuous Deployment geeignet sind, da diese in einer Zeit vor dem Continuous Deployment entstanden sind. Daher lassen sich neue Konzepte nur schwer auf diese Werkzeuge übertragen.

## 5 Fazit

DevOps ist kurz davor die Kluft für Marktakzeptanz zu überwinden, dies liegt an der steilen Anzahl von Materialien zu DevOps. Sobald DevOps normale Vorgehensweise in vielen Unternehmen ist, führt die gesteigerte Effektivität und Leistungssteigerung zur schnelleren Einführung von Softwareinnovationen in der Welt. Erfolgreiche Unternehmen wie Amazon, Google und Netflix, die DevOps in Verbindung der Microservice Architektur verwenden, lassen darauf schließen, dass in den nächsten Jahren DevOps von vielen weiteren Unternehmen eingeführt wird.