Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

CLOUD-BETRIEB IM ÖFFENTLICHEN SEKTOR: SELBSTBEDIENUNG, AUTOMATISIERT

Jan Gottschick, Uwe Holzmann-Kaiser, Holger Kurrek

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Jan Gottschick, Uwe Holzmann-Kaiser, Holger Kurrek

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-948582-05-0

1. Auflage Februar 2021

Fotonachweise:

Seiten	Autoren	Quellen
1	dimitrisvetsikas1969	pixabay.com
6	Monsterkoi	pixabay.com
10	ÖFIT	
17	photo-graphe	pixabay.com
22	anncapictures	pixabay.com
26	ÖFIT	
28	ÖFIT	
30	Love_and_Hope	pixabay.com

VORWORT

Die IT der öffentlichen Verwaltung muss die Erwartungen der Bürgerinnen und Bürger an ein zeitgemäßes Online-Angebot erfüllen, das klassische Behördengänge weitgehend ersetzt. Ein gelegentlich unterschätzter Aspekt für die Leistungsfähigkeit von IT ist die Gestaltung von Geschäftsprozessen zur Bereitstellung von Software. Eine schnelle Umsetzung des politischen Willens erfordert eine schnelle Bereitstellung neuer oder geänderter Software, ganz gleich ob für Nutzer:innen innerhalb oder außerhalb der Verwaltung. Damit diese Herausforderungen angegangen werden können, braucht es die Umsetzung zeitgemäßer Entwicklungs- und Betriebsmodelle der IT als solide Grundlage für die öffentliche Verwaltung.

Das vorliegende White Paper stellt den Betrieb moderner IT-Anwendungen in der Cloud in den Mittelpunkt. Die Nutzung von Cloud-Techniken folgt dabei nicht einem aktuellen Hype, sondern ermöglicht die Umsetzung der vielfältigen Anforderungen an aktuelle Software, die über die unmittelbare Funktionalität hinausgehen. Sicherlich lässt sich ein Fachverfahren mittels IT auf ganz unterschiedliche Weise realisieren, aber wenn es beispielsweise um Anpassungsfähigkeit an verschiedene Endgeräte, Skalierbarkeit bei schwankenden Nutzungszahlen oder auch um schnelle Anpassungen sowie kurze Entwicklungszyklen geht, dann spielt die Cloud ihre Vorteile aus. Die Cloud und damit einhergehende, moderne Entwicklungsmethoden wie »DevOps« können die Verwaltung aktiv dabei unterstützen, auch agiler zu werden.

Diese Publikation schafft zunächst ein gemeinsames Verständnis der Cloud-Technik: Worauf basiert sie technisch und wie wird sie bei der Bereitstellung von IT-Anwendungen (Deployment) genutzt? Der Einsatz der Cloud hat allerdings wesentlich weitreichendere Folgen als es zunächst scheint. Unterstützt wird nicht nur die agile Softwareentwicklung mit ihrem Grundprinzip »release early, release often«, sondern die Cloud fordert auch eine Automatisierung beim Betrieb von IT-Anwendungen.

Das White Paper zeigt auf, dass die Entwicklung und der Betrieb moderner IT-Anwendungen zu einem Kulturwandel führen – nicht nur innerhalb von Organisationen, sondern auch zwischen Organisationen. Rechenzentren und IT-Dienstleister der öffentlichen Verwaltung müssen sich im Laufe dieser Entwicklung stärker fokussieren und vor allem müssen auch ihre Mitarbeiter:innen neue Kompetenzen entwickeln. Und nicht zuletzt gilt es auch, sich mit dem Thema Digitale Souveränität in Bezug auf die IT- und Kommunikationsinfrastruktur auseinanderzusetzen.

Das White Paper richtet sich daher nicht nur an die konkret Verantwortlichen bei IT-Dienstleistern und ihren Kunden in der öffentlichen Verwaltung, sondern auch an die IT-Strateg:innen bei IT-Dienstleistern sowie in öffentlicher Verwaltung und Ministerien, die über die zukünftige Organisation von IT in Bund, Ländern und Kommunen oder gar EU-weit nachdenken. Das Papier soll aufrütteln, insbesondere im Hinblick auf die Organisation von IT-Dienstleistern und neue Kompetenzen der IT-Beschäftigten, und erste Lösungswege aufzeigen. Zentrale Begriffe und Konzepte werden im Anhang erläutert.

Die Autoren danken Klaus-Peter Eckert, Lena Farid und Jens Tiemann für inhaltliche Anregungen und Diskussionen.

Wir wünschen eine anregende Lektüre!

Ihr Kompetenzzentrum Öffentliche IT

FACHVERFAHREN SOLLEN GENAUSO ANSEHNLICH, KOMFORTABEL, PERFORMANT UND ZUVERLÄSSIG SEIN WIE BEKANNTE LÖSUNGEN DER INTERNET-ÖKONOMIE.

INHALTSVERZEICHNIS

1. THESEN

IT-Anwendungen müssen reaktiv, performant und verfügbar sein.
Die rasante Entwicklung des Internets und der dort verfügbaren Angebote setzt Standards und weckt Erwartungen an die Gestaltung und Leistungen von Web-Anwendungen – auch an die IT-Anwendungen, die intern in Organisationen und Unternehmen eingesetzt werden.

IT-Fachverfahren müssen zeitnah weiterentwickelt werden.
IT-Fachverfahren helfen der Verwaltung, ihre Aufgaben gesetzeskonform, fristgerecht und effizient umzusetzen. Diese Aufgaben unterliegen aber auch einem stetigen Wandel, beispielsweise durch Änderungen von Gesetzen und Vorschriften, der Rechtsprechung, der Verwaltungspraxis und vielem mehr.

Zukünftige IT-Fachverfahren benötigen Cloud-Technologien.
Die neuen Cloud-Technologien sind die Basis, um IT-Systeme zukünftig performanter, reaktiver, ausfallsicherer und zuverlässiger zu realisieren. Sie unterstützen ein agiles Vorgehen bei der Neuentwicklung von IT-Lösungen oder bei einem Redesign. Die Cloud-Technologien wie Container, Serverless Functions, Kubernetes und viele mehr bilden die notwendige Grundlage zukünftiger IT-Lösungen.

Der Betrieb von IT-Fachverfahren im eigenen Hoheitsgebiet ermöglicht maximale Informationssicherheit.
Grundsätze von Informationssicherheit und digitaler Souveränität verpflichten den deutschen Staat, seine eigenen Daten gegen den unberechtigten Zugriff Fremder zu schützen. Dies lässt sich vollumfänglich nur kontrollieren, wenn die digitalen Infrastrukturen (Kommunikationswege und Rechenzentren) des Staates innerhalb seines Hoheitsgebietes liegen und durch vertrauenswürdige Betreiber bereitgestellt werden, die ausschließlich der deutschen bzw. europäischen Gerichtsbarkeit und Kontrolle unterliegen.

Selbstbedienung ersetzt Change Requests und Tickets.
Das Management moderner Cloud-Lösungen sollte überwiegend durch den IT-Anwendungsbetrieb des Kunden und den Kunden selbst erfolgen können. Entsprechend stellt der Betreiber dem Kunden vorrangig Ressourcen wie Kommunikationswege, Rechen- und Speicherkapazitäten pauschal bereit, die dieser dann bei Bedarf im Rahmen seines Vertrages eigenständig abrufen kann.

Die Cloud kann nur disruptiv eingeführt werden.
Statt wie bisher ein fertiges Softwareprodukt mit einem Betriebshandbuch zu übergeben, damit ein Betreiber die entsprechende Software händisch installiert und für einen Kunden bereitstellt, gibt es einen automatischen, kontinuierlichen Bereitstellungsprozess (Staging) von der Entwicklung in die Vorprüfung, in die Abnahme – und letztendlich in die Produktivumgebung. Damit ändert sich die technische Umsetzung der Geschäftsprozesse des IT-Dienstleisters so radikal, dass eine behutsame Migration und Doppelstrukturen allenfalls kurzfristig sinnvoll sind.

IT-Dienstleister wie Rechenzentrumsbetreiber brauchen neue Fähigkeiten.
Obwohl die grundsätzliche Aufgabe, IT-Fachanwendungen auf einer gegebenen IT-Infrastruktur zu betreiben, für die Systemadministrator:innen bzw. Operator (kurz: Ops) gleichbleibt, ist es primär das Ziel, diese Aufgabe zu standardisieren und zu automatisieren (Provisioning). Die Tätigkeit des »Ops« verschiebt sich dadurch mehr in Richtung Softwareentwicklung bzw. Automatisierung zur Bereitstellung der (Cloud-)Infrastruktur (Infrastructure-as-Code). Diese neuen, notwendigen Fähigkeiten bedingen eine Anpassung der Organisation der Betreiber, sowohl hinsichtlich ihrer Strukturen als auch ihrer Kultur.

2. WANDEL DES IT-BETRIEBS

Die rasante Entwicklung des Internets und der dort verfügbaren Angebote, wie Suchmaschinen, Onlinehandel, Social Media, Spiele u. v. m. setzt Standards und weckt Erwartungen an die Gestaltung und Leistung von IT. Die Nutzer:innen können inzwischen mit Web-Anwendungen flüssig und ergonomisch arbeiten, ohne im Arbeitsfluss unterbrochen zu werden – vergleichbar mit lokalen IT-Anwendungen auf dem PC oder Apps auf dem Smartphone. Nutzer:innen haben auch den Anspruch, eine IT-Anwendung jederzeit nutzen zu können. Gleichzeitig steigen permanent die zu verarbeitenden Datenmengen, die durchzuführenden Aufgaben und Berechnungen werden umfangreicher. Diese Entwicklung erfordert eine leistungsfähige, effektive und effiziente Kommunikations- und Computing-Infrastruktur.

In den vergangenen Jahren hat mit den Cloud-Technologien in der IT ein Technologiesprung stattgefunden. Container zur Virtualisierung werden heute vor allem in Fachkreisen diskutiert, mit Begriffen wie Docker, OpenShift oder Kubernetes. Aber genau wie die Einführung von Containern im Warentransport ist die Container-Virtualisierung eine disruptive Technologie mit massiven Auswirkungen auf die Rechenzentren, die Softwareentwicklung und sogar die Nutzung von Software.

Die Entwicklung der Cloud beflügelt neue Konzepte in der Softwarearchitektur, um IT-Systeme modularer und flexibler zu designen sowie Software schneller zu realisieren. Die neuen Technologien sind vor allem aber die Basis, um IT-Systeme zukünftig performanter, reaktiver, ausfallsicherer und zuverlässiger zu machen. Sie unterstützen außerdem ein agiles Vorgehen bei der Entwicklung zukünftiger IT-Lösungen oder bei einem Redesign. Die Cloud-Technologien bilden die notwendige Grundlage für neue, innovative IT-Lösungen, die die oben genannten Erwartungen erfüllen können.

Container-Virtualisierung in Verbindung mit der Zerlegung komplexer Softwareanwendungen in Microservices bietet vielfältige neue Möglichkeiten zur Nachnutzung von Software. So brauchen in verschiedenen IT-Anwendungen benötigte Grundfunktionen (beispielsweise eine Stammdatenerfassung oder eine Suche) nur einmal entwickelt und gepflegt zu werden, um sie mehrfach zu nutzen. Schulungs- und Einarbeitungsaufwände werden reduziert, da die Nutzung ähnlicher Funktionen nicht für jede IT-Anwendung neu erlernt werden muss.

Vor allem Rechenzentren und IT-Dienstleister müssen sich diesem Wandel stellen und ihn gezielt für ihre Kunden einsetzen. Die Auswirkungen der Einführung der Cloud sind erheblich, und eine zeitgemäße IT-Infrastruktur ist eine zwingende Voraussetzung für moderne Softwarearchitekturen und wettbewerbsfähige Geschäftsprozesse. Für die Softwareentwicklung selbst sind Cloud-Lösungen lediglich ein normaler, evolutionärer Schritt im typischen Innovationszyklus. Für den IT-Betrieb dagegen ist die Einführung einer Container-basierten Cloud eine radikale Umstellung, sowohl aus technischer, organisatorischer, kultureller als auch aus geschäftlicher Sicht.

Virtualisierung

Die wesentliche Grundlage für die Cloud sind die Fortschritte in der Virtualisierung von IT-Ressourcen. Virtualisierung bedeutet, dass Nutzer:innen nicht mehr genau wissen, wo exakt in einem physischen System wann was berechnet wird, wo welche Daten gespeichert werden, oder welchen Weg Daten in einem Netzwerk nehmen.[1]

Der erste Schritt war, dass sich Nutzer:innen einen Computer innerhalb eines Betriebssystems »teilen« konnten, d. h. alle Nutzer:innen haben den Eindruck, einen Rechner für sich allein zu haben. Ein weiterer Schritt waren Virtuelle Netze (VPN), durch die Computer auch standortübergreifend untereinander vernetzt und gleichzeitig gegen andere Netze sicher abgeschottet werden können, obwohl sie sich ein physisches Netz teilen bzw. das Internet nutzen.

Aus der Möglichkeit, einen physischen Rechner quasi auf der Hardware-Ebene zu teilen und den Nutzer:innen mehrere virtuelle Maschinen bereitstellen zu können, entstand das heute gängige Angebot Infrastructure-as-a-Service (IaaS). Kunden können vorkonfektionierte und damit kostengünstig bereitgestellte virtuelle Rechner und Netze per »Knopfdruck« mieten und sofort nutzen. Entscheidend ist, dass die Kunden auf einer virtuellen Maschine ihr präferiertes Betriebssystem nutzen und selbst verwalten können. Wo sich die physischen Rechner konkret befinden, ist für den Kunden dagegen irrelevant.

[1] Im Gegensatz zu den Nutzer:innen können Systemadministrator:innen die Nutzung konkreter IT-Ressourcen und Kommunikationsverbindungen nachvollziehen bzw. steuern.

CONTAINER-VIRTUALISIERUNG IST EINE DISRUPTIVE TECHNOLOGIE MIT AUSWIRKUNGEN AUF RECHENZENTREN, SOFTWAREENTWICKLUNG UND SOGAR DIE NUTZUNG VON SOFTWARE.

Der für das heutige Verständnis von Cloud nächste und wichtigste Schritt ist die Container-Technologie [12], die eine noch bessere Auslastung der Computing-Ressourcen erlaubt. Das Cloud-Angebot Container-as-a-Service (CaaS) erlaubt heute die effektive und effiziente Orchestrierung einer großen Anzahl an Containern auf Basis des Industriestandards Kubernetes (K8s) [10]. Kubernetes lässt sich also als »Betriebssystem der Cloud« verstehen.

Container – eine Analogie

Während Frachtcontainer den Laderaum eines Schiffes in genormt von Kunden nutzbare Großraumbehälter aufteilen, bietet Container-Virtualisierung eine Nutzung von physischer Computerhardware in Form von virtuellen Ablaufumgebungen für Software, also quasi »kleinen Computern« bzw. »Servern«. Dadurch können für unterschiedliche IT-Anwendungen jeweils voneinander separierte und mit definierten Ressourcen wie Rechen- und Speicherkapazität ausgestattete einzelne virtuelle »Computer« bzw. »Server« bereitgestellt werden. Im Vergleich zu virtuellen Maschinen können durch Container auch für kleinere Softwareteile separate Umgebungen effektiv erzeugt und betrieben werden. Genau wie für Frachtcontainer genormte Halterungen definiert sind, bieten virtuelle Container definierte Konfigurationsmöglichkeiten zum Einsatz von Software.

Bei Frachtcontainern erfolgt die Beladung mit Waren nicht mehr durch Personal am Schiff, sondern vorher beim Absender. So wie bei der Beladung mit Containern am Schiff laufen bei Container-Virtualisierung in Rechenzentren nur noch standardisierte und automatisierte Installationsprozesse ab. Bereits durch die Softwareentwickler werden auch die Installation (Deployment) und der Betrieb von IT mitgeplant und nicht mehr allein dem Personal im Rechenzentrum überlassen. Softwareentwicklung (Development) und IT-Betrieb (IT-Operations) werden zusammengeführt zu DevOps. Die IT-Dienstleister mit ihren Rechenzentren können sich auf die Bereitstellung (Provisioning) von IT-Ressourcen (Rechenkapazitäten, Speicher und Netze) und standardisierter Installation (Deployment) in definierten IT-Infrastrukturen (Container-as-a-Service, CaaS, aber auch Infrastructure-as-a-Service, IaaS) konzentrieren. Softwareentwickler:innen übernehmen die korrekte Konfiguration und integrieren auch automatisierte Reaktionen auf Fehlerzustände in ihre Software.

Genau wie vor Jahrzehnten bei Frachtcontainern kann die Container-Virtualisierung bei richtiger Anwendung zu einer Verringerung der Kosten für den IT-Betrieb und einer Beschleunigung der Betriebsprozesse führen. Dabei wandeln sich auch die Berufsbilder in Rechenzentren, genau wie die Frachtcontainer zu vollautomatisierten Containerhäfen mit entsprechend neuen Berufsbildern führten.

Frachtcontainer haben durch schnelleren Warentransport bzw. -umschlag moderne Lieferketten ermöglicht. Die Container-Virtualisierung beschleunigt durch Automatisierung die zeitnahe Verbesserung von Software (Updates), sodass eine fortlaufende Optimierung des Nutzungserlebnisses (User Experience) für die Nutzer:innen von Geschäftsprozessen ermöglicht wird. Agile Softwareentwicklung wird möglich, bei der häufiger neue Versionen in kürzeren Abständen produktiv bereitgestellt werden und damit schneller auf Kundenwünsche reagiert werden kann.

Moderne Softwareentwicklung

Die Cloud-Technologien haben auch einen Einfluss auf die Entwicklung von Software und den Umgang mit ihr sowie auf die zeitnahe Umsetzung neuer Geschäftsprozesse und Geschäftsideen. Bei modernen, nativ digitalen Unternehmen treibt die IT die Geschäftsmodelle. Bei klassischen Organisationen werden dagegen oft lediglich existierende Geschäftsprozesse digitalisiert. Technisch stellt die Cloud beispielsweise auch eine neue Variante der Dienstplattform (Service-oriented Architecture, SoA 2.0) dar und hilft, moderne Softwarearchitekturen wie Microservices [6] und Self-Contained Systems [8] technisch zu realisieren und zu betreiben.

Abbildung 1: Klassische Übergabe von Software

IT-Fachverfahren helfen der Verwaltung, ihre Aufgaben gesetzeskonform, fristgerecht und effizient umzusetzen. Durch Änderungen von Gesetzen und Vorschriften, Rechtsprechung, der Verwaltungspraxis u. v. m unterliegen auch die Aufgaben der Verwaltung einem stetigen Wandel. Entsprechend müssen die IT-Fachverfahren aus fachlichen Gründen, auf Basis von Nutzeranforderungen oder zur Verbesserung der Bedienbarkeit regelmäßig angepasst werden. Zudem entwickelt sich die IT-Technologie fortlaufend weiter. Dadurch sind Änderungen und Überarbeitungen der IT-Fachverfahren unabdingbar, um nicht zu veralten und ineffektiv zu werden oder um neue Sicherheitsanforderungen zu erfüllen. Die Erstellung von IT-Fachverfahren ist somit kein einmaliges Projekt. Ein IT-Fachverfahren benötigt permanente Pflege, eine dauerhafte Aufgabe, die mal mehr und mal weniger Aufwand bedeutet. Dabei führen die hohen Anforderungen dazu, dass IT-Fachverfahren häufiger als bisher aktualisiert werden müssen und daher das Deployment zeitnah erfolgen muss.

Komplementär zur Einführung der Cloud-Technologien haben sich die Software-Entwicklungsmethoden weiterentwickelt. Insbesondere die agile Entwicklung und das Domain-Driven Design (DDD) [9] definieren neue Zuständigkeitsgrenzen im Entwicklungsprozess. Diese Entwicklung ist die Motivation für einen Continuous Integration / Continuous Deployment bzw. Delivery Prozess (kurz CI/CD). Bisher wurde das fertige Softwareprodukt dem Rechenzentrumsbetrieb inklusive eines Betriebshandbuches übergeben, damit dieser die entsprechende Software installiert und betreibt. Für die moderne IT-Anwendungsentwicklung bietet sich die Nutzung eines kontinuierlichen, durchgängigen Bereitstellungsprozesses (CI/CD, Staging) an, der von der Entwicklung in die Test-, in die Abnahme-, in die Schulungs- und bis letztendlich in die Produktivumgebung reicht. Durch die damit einhergehende Automatisierung des IT-Betriebes bedeutet dies für die IT-Dienstleister eine radikale Veränderung ihrer Dienstleistung, da diese einen anderen Fokus bekommt.

Auswirkungen auf IT-Dienstleister

Bisherige IT-Systeme werden vielfach noch weitgehend manuell verwaltet und betrieben, beispielsweise mithilfe eines Betriebshandbuches. Die komplexeren Cloud-basierten Lösungen müssen dagegen automatisiert installiert und betrieben werden können. Die Überwachung und Pflege sollte überwiegend durch den IT-Anwendungsbetrieb des Kunden und den Kunden selbst erfolgen können. Entsprechend stellt der Betreiber vorrangig Ressourcen wie Kommunikationswege, Rechen- und Speicherkapazitäten dem Kunden pauschal bereit, die dieser dann bei Bedarf im Rahmen seines Vertrages eigenständig abrufen kann. Der Abruf einzelner Ressourcen im Rahmen des vereinbarten Umfangs erfolgt dann in einem Selbstbedienungsportal und nicht mehr manuell per Change Request bzw. Ticket an den Betreiber.

Bisherige manuelle Tätigkeiten beim Betreiber der Ressourcen werden durch Code (Infrastructure-as-Code, IaC) [11] ersetzt. Zwar gibt es hierfür Werkzeuge, aber die Tätigkeit des »Ops« verschiebt sich dadurch in Richtung Automatisierung und Softwareentwicklung. Der Betreiber ist somit nur noch für die Funktionsfähigkeit und rechtzeitige, proaktive Bereitstellung der Ressourcen verantwortlich. Die Funktionsfähigkeit des IT-Fachverfahrens selbst wird durch den IT-Anwendungsbetrieb des Kunden gewährleistet.

3. MODERNE ANSÄTZE FÜR IT-DIENSTLEISTER

So alt wie der Computer selbst ist auch der Betrieb von IT-Ressourcen. Klassischerweise werden die IT-Anwendungen von Softwareentwicklern erstellt, von Systemadministrator:innen auf den Computern installiert und die Nutzer:innen der IT-Anwendungen hoffen, mit der Lösung ihre Aufgaben erledigen zu können. Dabei hat sich die Arbeit der Administrator:innen über die Jahrzehnte kaum verändert. Die Entwickler:innen liefern die Software auf einem (virtuellen) Datenträger in Binärform und eventuell als Quellcode sowie eine mehr oder weniger präzise Installations- und Betriebsanleitung (Betriebshandbuch). Auf dieser Grundlage müssen die Administrator:innen zusehen, wie die IT-Anwendungen auf den Systemen »zum Laufen« gebracht werden können.

Insbesondere im Consumer-Bereich und vor allem bei mobilen Endgeräten gibt es heute ausgefeilte Installationswerkzeuge (Appstore), die eine Bereitstellung von IT-Anwendungen (Deployment) weitestgehend automatisiert durchführen. Dagegen ist bei einigen IT-Dienstleistern die Installation von IT-Anwendungen noch »Handarbeit«. Erst mit der Cloud und agilen Entwicklungsmethoden haben sich Verantwortlichkeiten und Prozesse für das Deployment (also die Installation bzw. das Ausrollen von Software) in Rechenzentren nachhaltig verändert. Insbesondere große Cloud-Anbieter (Hyperscaler) fokussieren sich auf die reine Bereitstellung von IT-Ressourcen (Provisioning), wie Rechenkapazität, Speicher und Kommunikationsnetze sowie grundlegender Dienste. Bei diesen IT-Dienstleistern gibt es keine Administrator:innen mehr, die das Deployment händisch unterstützen. Das Deployment der IT-Anwendung obliegt der/dem Verantwortlichen für die IT-Anwendung selbst.

Mit dem aus agilen Methoden entstandenen »DevOps-Prinzip« sind die Softwareentwickler:innen verstärkt in der Pflicht, die Installation und den Betrieb ihrer entwickelten IT-Anwendung inklusive des Monitorings der IT-Anwendung (Fehler- und Problemerkennung, Erfassung von Daten zur Optimierung) zu gewährleisten, d. h. diese Aufgaben idealerweise durch Automatisierung der zugehörigen Prozesse zu realisieren. Der produktive Betrieb von IT-Anwendungen wird entsprechend zunehmend durch ergänzende, für die IT-Anwendung spezifische Operator-Software ebenfalls teilautomatisiert.

3.1 DIE ROLLE DER ÖFFENTLICHEN IT-DIENSTLEISTER

Grundsätze von Informationssicherheit, Datenschutz bis zu digitaler Souveränität verpflichten den deutschen Staat, seine eigenen Daten gegen den unberechtigten Zugriff Fremder zu schützen. Die Hintergründe können vielfältig sein, von staatlicher Geheimhaltung über den Schutz geistigen Eigentums von Wirtschaftsunternehmen bis zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSGVO).

Die Staatsgewalt sowie die staatliche, hoheitliche Zuständigkeit beziehen sich bisher auf das geografische Territorium eines modernen Staates. Das Territorium erschließt einen physischen Raum mit klaren geografischen Grenzen, die kartografiert und markiert sind. »Die rechtliche Grundlage für die räumliche Gliederung der Verwaltung ist das sogenannte Territorialprinzip. Es besagt, dass der Wirkungskreis eines Organs nach örtlichen Grenzen abgesteckt wird; für das Handeln der Behörde bzw. des Organs wird mithin auf ein bestimmtes Territorium, insbesondere auf einen bestimmten Teil des Staatgebietes abgestellt.« [2]

In der »analogen Welt« ist das Hoheitsgebiet, in dem ein Staat seine Staatsmacht ausübt und seine Zuständigkeiten regelt, durch Grenzen relativ klar auf einen geografischen Raum beschränkt. In der »digitalen Welt« ist die Zuordnung von digitalen Räumen zu geografischen Räumen aufgrund der Vernetzung und der Virtualisierung von Kommunikationswegen, Rechnern und Speicherorten nicht mehr eindeutig. Damit ist auch die Zuständigkeit für bzw. Hoheit über Daten mitunter schwer eingrenzbar. Weiterhin ist zu berücksichtigen, dass in der »digitalen Welt« Eigentumsverhältnisse, Datenzugriff durch Dritte (international) und Datenschutz neu interpretiert und auch rechtlich unterschiedlich gehandhabt werden. So gibt es Staaten, die eine Hoheit über Daten an den Betreiber der Infrastruktur koppeln. In diesem Fall hat ein (fremder) Staat die Hoheit über alle Daten des Betreibers, sofern der Betreiber der Gerichtsbarkeit des Staats unterliegt, selbst wenn die Daten nicht dem Betreiber, sondern Dritten bzw. seinen Kunden gehören. [7]

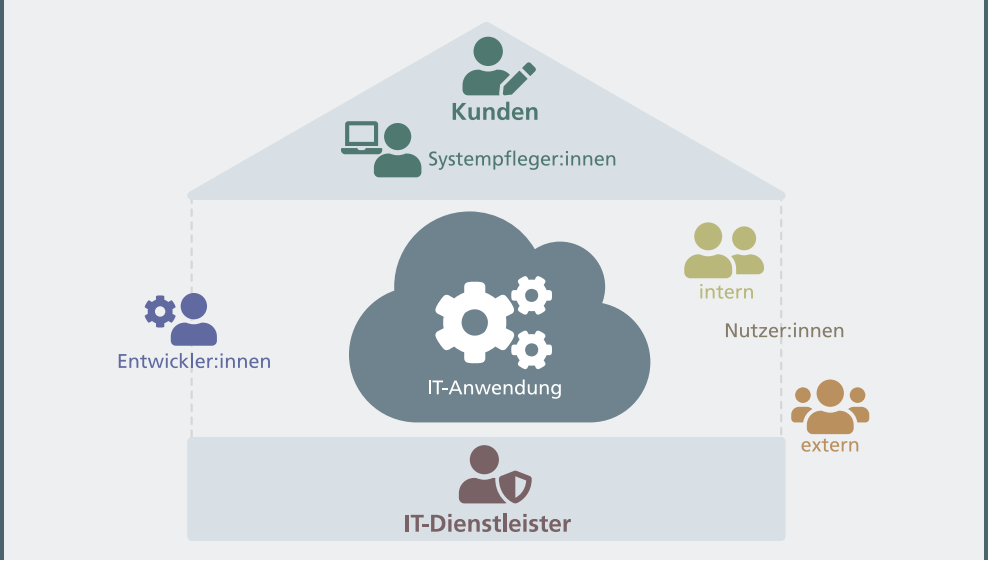


Abbildung 2: Rollen bei der Cloud-Nutzung

Die digitale Infrastruktur muss einen (ungewollten oder unberechtigten) Abfluss der Daten effektiv verhindern. Dies lässt sich leichter gewährleisten, wenn die Infrastruktur (Kommunikationswege, Rechenzentren usw.) des Staates letztlich komplett innerhalb seines Hoheitsgebietes liegt und durch einen vertrauenswürdigen Betreiber bzw. öffentlichen Dienstleister bereitgestellt wird, der ausschließlich der Hoheit des deutschen Staates und seiner Gerichtsbarkeit unterliegt. Aus der Perspektive Deutschlands bietet auch eine Infrastruktur innerhalb der Europäischen Union (EU) und deren digitalem Raum Vorteile. Auf Basis einer Risikoanalyse kann fallbezogen entschieden werden, welcher Grad von territorialer Hoheit über die Infrastruktur zielführend ist und inwieweit die Anwendung des Territorialprinzips vor dem Hintergrund der jeweiligen Anforderungen technisch realisierbar ist.[2]

Technisch und organisatorisch kann ein IT-Dienstleister sein Cloud-Angebot natürlich nicht nur auf eigenen IT-Ressourcen aufbauen, sondern mittels Multi-Cloud- und Hybrid-Cloud-Lösungen je nach technischen Anforderungen und erforderlichem Schutzniveau externe IT-Ressourcen von anderen öffentlichen, aber auch kommerziellen IT-Dienstleistern in seine Dienstleistung einbinden. Dies ermöglicht wirtschaftlichere Angebote, IT-Ressourcen bei einem kurzfristigen Bedarf flexibler bereitzustellen und frühzeitig innovative Technologien verfügbar zu machen. Ein Outsourcing, ein Betrieb von nicht sicherheitszertifizierter Hard- und Software oder ein Betrieb durch nicht vertrauenswürdiges Personal ist ein erhöhtes Sicherheitsrisiko.

[2] Diese pauschale Betrachtung findet natürlich auch keine Anwendung bei Verfahren, bei denen zwischen Staaten im Einzelfall Daten bei einem begründeten Interesse und zweckbeschränkt legal ausgetauscht werden dürfen. Hier sind verfahrensspezifische Regelungen zu treffen unter Berücksichtigung des jeweiligen digitalen Raumes.

3.2 ERWARTUNGEN VON IT-ANWENDERN

Wer sind eigentlich Anwender, Entwickler und Betreiber der IT-Anwendungen im öffentlichen Bereich? Dies hängt von der konkreten IT-Anwendung ab. Im Kontext dieser Betrachtung kann man generell folgende beteiligte Gruppen bzw. Rollen identifizieren (siehe Abbildung):

- Nutzer:innen
  - interne Nutzer:innen innerhalb einer Organisation (Verwaltung)
  - externe Nutzer:innen (z. B. Bürger:innen, Wirtschaft und andere Behörden)
- Kunden (Verantwortliche für die IT-Anwendungen, auch Verantwortliche im Sinne der DSGVO, Auftraggeber für IT-Dienstleister)
  - Systempfleger:innen (fachliche Administration für eine IT-Anwendung innerhalb der Organisation)
- Entwickler:innen (interne oder externe Softwareentwickler:innen der IT-Anwendung)
- IT-Dienstleister (verantwortlicher Betreiber der IT-Ressourcen)

Systempfleger:in bezeichnet die Rolle des Bindeglieds zwischen der fachlich-politischen Verantwortung und der technisch-betrieblichen Durchführung, mit dem Wissen um fachlich-technische Zusammenhänge einer IT-Anwendung.

Die Nutzer:innen wollen mit IT-Anwendungen jederzeit schnell und effektiv arbeiten, Aufgaben erledigen bzw. konsumieren können. Die Bedienung selbst soll natürlich komfortabel, barrierefrei und einfach sein. Kunden bzw. Verantwortliche für eine IT-Anwendung wollen diese kostengünstig nutzbar machen (gegenüber internen oder externen Nutzer:innen) und pflegen können. Dabei muss garantiert sein, dass die durch Nutzer:innen erzeugte Last auf die IT-Anwendung jederzeit mittels der vorhandenen IT-Ressourcen bewältigt werden kann und dass die IT-Anwendung möglichst nie ausfällt.

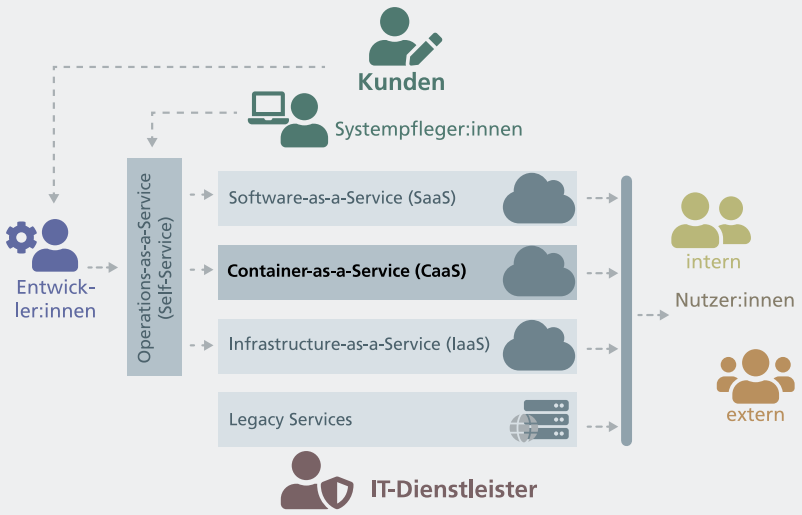


Abbildung 3: Cloud-Umgebung

Die sich daraus ergebenden technischen Anforderungen an die IT-Anwendung und deren Betriebsumgebung spiegelt »Das Reaktive Manifest«[3] sehr gut wider:

- Antwortbereit (responsive): »Das System antwortet unter allen Umständen zeitgerecht, […]«
- Widerstandsfähig (resilient): »Das System bleibt selbst bei Ausfällen von Hard- oder Software antwortbereit.«
- Elastisch (elastic): »Das System bleibt auch unter sich ändernden Lastbedingungen antwortbereit. […] Bei Verminderung oder Erhöhung der Last werden automatisch die Replizierungsfaktoren und damit die genutzten Ressourcen angepasst.«

Pragmatisch ausgedrückt sollten die IT-Anwendungen der Verwaltung genauso ansehnlich, komfortabel, performant und zuverlässig sein wie die Lösungen der Giganten der Internetökonomie.

3.3 DIE CLOUD AUS TECHNISCHER SICHT

Der Begriff Cloud wird in der Praxis sehr unterschiedlich verwendet [4], bspw. bei (mobilen) Endgeräten für das Speichern oder Verteilen von Daten »im Internet« (Dropbox, Google Drive, iCloud, ownCloud usw.) oder für das Verlagern einer kompletten Unternehmens-IT zu spezialisierten Dienstleistern für den professionellen Betrieb von IT-Ressourcen (Public Cloud) [5].

Technologisch basieren moderne Cloud-Infrastrukturen vor allem auf Containern (Container-as-a-Service, CaaS) und Funktionen (Function-as-a-Service, FaaS), die jeweils in einer spezifischen Art und Weise die Funktionalitäten einer IT-Anwendung realisieren. Container und Funktionen sind meist effizienter und effektiver als virtuelle Maschinen (Infrastructure-as-a-Service, IaaS), die in einigen Anwendungsfällen aber auch Vorteile haben, notwendig sind und ergänzend bereitstehen sollten. Die effizientere Ausnutzung der IT-Ressourcen von Virtualisierungslösungen sollte sich letztlich auch in niedrigeren Betriebskosten niederschlagen. Weiterhin vermeidet die Kapselung der Container Installationskonflikte, wie sie auf gemeinsam verwendeten physischen Rechnern und virtuellen Maschinen auftreten.

Die Container und Funktionen werden von einer Container-Orchestrierung wie der offenen Plattform Kubernetes verwaltet. Als Betriebssystem für die Cloud-Infrastruktur verstanden, bündelt Kubernetes dazu gemeinsam verwaltete Container in einem Container-Cluster. Die Cluster werden untereinander streng abgeschottet. Kubernetes instanziiert die Container in den Clustern, sorgt für die notwendige Skalierung der IT-Anwendung und verwaltet sowohl die Cloud-Anwendungen als auch benötigte Ressourcen. Damit kann die Last von IT-Anwendungen automatisch verteilt und die IT-Anwendungen können redundant zur Verfügung gestellt werden. Bei klassischen Infrastrukturen mit physischen oder virtuellen Maschinen muss dies separat und eigenständig gelöst werden.

Eine Cloud-Umgebung muss aber auch von allen Kunden benötigte Dienste bereitstellen (Software-as-a-Service, SaaS), also bspw. Objektspeicher und Sicherheitsfunktionen. Ferner muss auch auf bestehende, noch in Betrieb befindliche Dienste (Legacy Services) zugegriffen werden können. Die/der Systempfleger:in des Kunden kann die IT-Anwendungen und die benötigten IT-Ressourcen über das Selbstbedienungsportal (Operations-as-a-Service, OaaS) selbstständig verwalten.

Damit eine IT-Anwendung in der Cloud effektiv funktioniert, wird sie auf Basis spezifischer Softwarearchitekturen und IT-Paradigmen entwickelt. Beispiele sind Service-oriented Architecture (SOA), Microservices, Self-Contained Systems, Reactive Systems, Domain-Driven Design u. v. m.

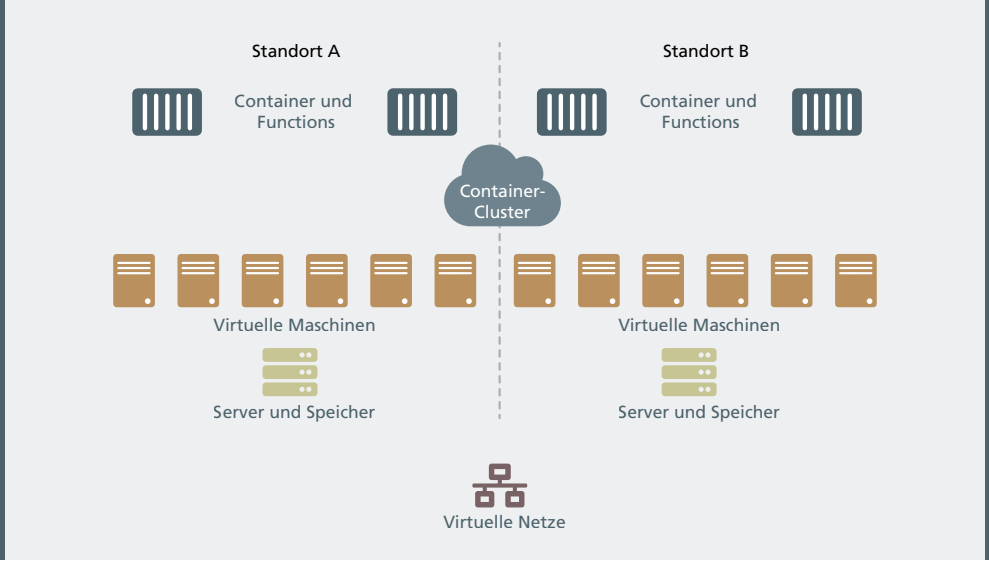


Abbildung 4: Technische Cloud-Infrastruktur

In Abbildung 4 ist eine typische technische Cloud-Infrastruktur skizziert. Neben den Netzwerken mit ihren virtuellen Netzen bilden die physischen Server und deren Speichersysteme die technische Basis. Generell wird eine Cloud-Infrastruktur immer auch redundant auf mehrere Standorte verteilt. Dies kann einerseits auf mehrere, separate Rechenzentren (Availability Zone, AZ) und andererseits auf weit entfernte Standorte (Regions) erfolgen. Die Redundanz dient sowohl einer höheren Verfügbarkeit als auch einer besseren Lastverteilung. Aufbauend auf den physischen Systemen können virtuelle Maschinen (IaaS) und Container-Cluster zur Ausführung von Containern (CaaS) und Functions (FaaS) standortübergreifend erstellt werden.

Zusammengefasst ermöglicht die Cloud-Infrastruktur als CaaS-Cloud, die IT-Ressourcen effizient zu nutzen, die IT-Anwendungen reaktiv, widerstandsfähig und elastisch zu machen sowie die Komplexität für den Betrieb aber auch die Softwareentwicklung selbst zu beherrschen. Ob sich dabei mehrere Kunden (Mandanten) ein Cluster insbesondere in der Produktionsumgebung teilen können, ist nicht nur eine technische, wirtschaftliche und organisatorische Frage, sondern vor allem auch abhängig vom Schutzbedarf und dem Schutzniveau der konkreten IT-Anwendungen.

3.4 BEREITSTELLUNG VON IT-ANWENDUNGEN

Die Bereitstellung der IT-Anwendungen (Deployment) muss die internen Prozesse der öffentlichen Verwaltung beachten und folgt den Schritten Vorprüfung ► Abnahme ► Schulung ► Produktion. Grundsätzlich sollen alle Prozesse der Bereitstellung für den jeweiligen Schritt vollautomatisiert ablaufen. Nachfolgende Prozessschritte werden meist erst nach einer Freigabe durch die/den Verfahrensverantwortliche:n gestartet, wobei dies beispielsweise durch die/den Systempfleger:in im Selbstbedienungsportal erfolgen sollte.

Aus Sicht des Cloud-Betreibers werden IT-Anwendungen in der Cloud durch den Kunden in Form von einem oder mehreren Containern eines Clusters bereitgestellt. Grundsätzlich besteht eine Deployment-Umgebung minimal aus einem Cluster mit seinen zugehörigen IT-Ressourcen oder aber auch aus mehreren Clustern, um die verschiedenen Prozessschritte (Stages) voneinander unabhängig umsetzen zu können. Um die Software medienbruchfrei vom externen Kunden bzw. von den Softwareentwickler:innen sicher übernehmen zu können, werden Versionsverwaltungssysteme (Version Control System, VCS) eingesetzt. Es gibt es ein äußeres Versionsverwaltungssystem (VCS <A> in Abbildung 6), das aus dem Internet erreichbar ist, sowie ein inneres Versionsverwaltungssystem (VCS <B>), in das nur sicherheitsgeprüfte und integritätsgesicherte Dateien von zertifizierten Absendern nach einer Sicherheitsüberprüfung

Abbildung 5: Deployment-Prozess

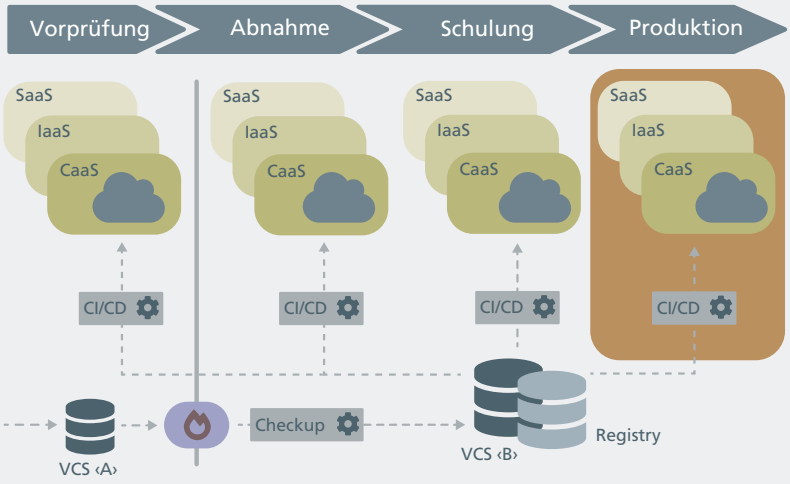


Abbildung 6: Deployment-Umgebung

(Checkup) übernommen werden. Ein betreiberspezifischer CI/CD-Prozess erzeugt aus den vorübersetzten Quelldateien die notwendigen Container-Images, speichert diese in einer eigenen, gesicherten Container-Registry und nutzt diese zur Instanziierung in den verschiedenen Clustern.[3]

Das Versionsverwaltungssystem (typischerweise Git, https://git-scm.com/) verwaltet die von den Entwickler:innen bereitgestellten Software-Artefakte. Diese umfassen die Dokumentation, die installierbaren Dateien, CI/CD-Konfigurationsinformationen/-skripte und ggf. auch den Quellcode (soweit vertraglich vereinbart). Ist der Quellcode verfügbar, so kann er bei Bedarf im Rahmen der Abnahme durch interne Werkzeuge qualitätsgesichert und auf Sicherheitslücken überprüft werden. Die installierbaren Dateien müssen fertig vorab übersetzt geliefert werden, d. h. als Binärdateien einzeln oder als lokales Distributionspaket, da der IT-Dienstleister letztlich nicht alle für die Erzeugung der Binärdateien notwendigen Entwicklungswerkzeuge in allen Versionsständen vorhalten kann. Es muss allerdings sichergestellt werden, dass der Quellcode und die Binärdateien zueinander passen. Beispielsweise müssen auch die notwendigen Skripte und die Dokumentation zur Generierung der Binärdateien vorliegen.

Die CI/CD-Konfigurationsinformationen dienen dem IT-Dienstleister dazu, die Images für die Container selbstständig in sicherer Form zu generieren und zu deployen. Dazu muss es detaillierte Vorgaben vom IT-Dienstleister geben, wie die CI/CD-Konfigurationsinformationen aufzubauen sind, damit die Container-Generierung, die Anpassung an die konkrete Cluster-Umgebung und die eigentliche Installation im Cluster vollautomatisch erfolgen können.

Der/die Softwareentwickler:in stellt die Software-Lieferung im äußeren Versionsverwaltungssystem VCS <A> in gesicherter Form (bspw. durch Prüfsummen, signiert usw.) dem Kunden zur Verfügung. Von dort kann der Kunde (bspw. durch den/die Systempfleger:in) die Lieferung in das innere Versionsverwaltungssystem VCS <B> übernehmen, wobei automatisch eine Sicherheitsüberprüfung (bspw. auf Viren) der Lieferung erfolgt. In der Vorprüfungs-Umgebung können die Entwickler:innen in eingeschränktem Rahmen ihre Software und das Deployment selbst testen. Die Einschränkungen bestehen in der Regel darin, dass eigene Testdaten benötigt werden und Dienste durch Mockups simuliert werden müssen, da diese nur in der Produktionsumgebung verfügbar sind (beispielsweise Authentifizierungssysteme mit realen Nutzer:innen). Die Tests sollten auch vollautomatisch erfolgen können. Nun kann die Lieferung nach der Freigabe durch die/den Systempfleger:in schrittweise in die verschiedenen internen Cluster automatisiert mittels der CI/CD-Konfigurationsinformationen deployed werden.

Das geschilderte Vorgehen stellt sicher, dass sowohl technische als auch organisatorische Rahmenbedingungen eingehalten werden. Die Automatisierung spart nicht nur Personalressourcen, sondern beschleunigt den Prozess erheblich und gestaltet diesen für Entwickler, Kunde und Betreiber nachvollziehbar.

3.5 NUTZUNG DER CLOUD DURCH KUNDEN

Im Zeitalter der Internetökonomie werden immer mehr digitale Dienstleistungen in Selbstbedienung angeboten. Diesem Trend kann sich die Verwaltung nicht verschließen. Durch Selbstbedienung sollen sowohl beim Kunden als auch beim IT-Dienstleister Kosten eingespart werden, wobei die Einsparungen von beiden für verbesserte Angebote genutzt werden können. Durch Selbstbedienung sollen vor allem auch die Entwicklungsprozesse organisatorisch effektiver gestaltet werden. Damit ein Entwicklungsteam vollständig die fachliche und technische Ver-

[3] In diesem Kontext ist mit CI/CD Continuous Integration/Continuous Deployment gemeint, wobei CI sich vor allem auf das Testen eines erfolgreichen Deployments bezieht. Die Softwareentwickler:innen nutzen ebenfalls einen CI/CD-Prozess, womit aber Continuous Integration/Continuous Delivery gemeint ist und CI sich auf das Testen der Softwarefunktionalität/-qualität bezieht.

SELBSTBEDIENUNG BEI IT-DIENSTLEISTUNGEN ERMÖGLICHT JEDERZEIT ZEITNAHEN UND BEDARFSGERECHTEN ABRUF.

antwortung für eine IT-Anwendung übernehmen kann, muss es alle Schritte von der Konzeption über die Entwicklung, die Bereitstellung, Überwachung und Pflege selbstständig und zeitnah durchführen können, ohne von Dritten abhängig zu sein.

Die globalen Cloud-Anbieter (Hyperscaler) demonstrieren erfolgreich diesen Weg, bei dem die Dienstleistungen in standardisierter, vorkonfektionierter Form, vollständig automatisiert und in Selbstbedienung verfügbar sind. Die Kommunikation zwischen IT-Dienstleister und Kunden wird minimiert und fokussiert sich einerseits auf die Schulung der Kunden und andererseits auf den gemeinschaftlichen Austausch mit den Kunden, um das eigene Angebot weiter zu entwickeln.

Die Kommunikation via Ticket-System und Change Requests ist bei Problemfällen (»Trouble Ticket«) sinnvoll, verursacht aber hohe Kosten und ist ineffizient. Alternativ können ein frühzeitiges Erkennen von Problemen und proaktives Handeln zusammen mit einer durchdachten Automatisierung die Prozesse beschleunigen und unnötige Kommunikationsvorfälle minimieren. Zu diesem Zweck liefert der Kunde dem IT-Dienstleister zukünftig neben der IT-Anwendung ergänzend auch noch eine Operator-Software, die betriebliche Standardaufgaben und Problembehandlung (Day-2 Operations, beispielsweise Fehlererkennung und -eskalation, Datensicherung und -wiederherstellung) für die zugehörige IT-Anwendung selbstständig durchführt, wodurch ein manueller Eingriff durch Systemadministrator:innen kaum noch notwendig ist.

Eine grundlegende Voraussetzung hierfür ist das Angebot des IT-Dienstleisters. Das Kernangebot muss einen standardisierten Umfang haben, wie beispielsweise das Buchen der IT-Ressourcen, grundlegender Dienste und von Sicherheitsfunktionen. Darüber hinaus sollte es ergänzend eine Anzahl von Mehrwertdiensten geben, die notwendige und gewünschte Anforderungen des Kunden sinnvoll abdecken sowie das Kernangebot zweckmäßig ergänzen.

Für die Kunden ist es sinnvoll, wenn die Kostenverrechnung der Dienstleistungen intern über einen haushaltstechnischen, vereinbarten Rahmen (Kontingent) erfolgen kann (im Gegensatz zu manchen Angeboten von kommerziellen IT-Dienstleistern, die über eine Kreditkarte abgerechnet werden). Ferner müssen die maximalen Kosten für die Kunden planbar sein.

Technisch werden die standardisierten Angebote den Kunden in Form einer Programmierschnittstelle zur Verfügung gestellt (API-First-Prinzip). Ergänzend gibt es ein Selbstbedienungsportal, es integriert Funktionen der Kundenverwaltung (Abrechnungen, Statusinformationen usw.) und das Buchen von IT-Ressourcen für IT-Fachverfahren. Kundenfreundlich ausgelegt, dient das Portal vorrangig zur grundlegenden Administration der IT-Ressourcen durch die Kunden selbst und zur Kommunikation zwischen Kunden und IT-Dienstleister. Die Programmierschnittstelle, ggf. ergänzt um zusätzliche Werkzeuge (Command-Line-Werkzeuge, CLI), unterstützt die Routine-Arbeiten der Entwickler:innen und des/der Systempflegers/in bzw. Anwendungssupports und erlaubt eine medienbruchfreie Automatisierung der Prozesse aufseiten der Kunden.

Zusammenfassend ermöglicht die Selbstbedienung der Dienstleistungen, dass diese jederzeit und zeitnah abgerufen werden können, sobald es eine Dienstleistungsvereinbarung gibt, die das Kontingent für die IT-Ressourcen und die Nutzung der Dienste definiert.

4. HANDLUNGSEMPFEHLUNGEN

Bei der Umsetzung der vorgestellten Ansätze zur Bereitstellung von IT-Anwendungen (Deployment) aus diesem White Paper sollen die nachfolgenden Handlungsempfehlungen helfen, die als Grundlage für einen vollständigen Fahrplan zur erfolgreichen Umsetzung eines modernen Systembetriebs dienen können.

Die Deployment-Umgebung technologisch modernisieren.

Die Kernaufgabe eines IT-Dienstleisters ist die effiziente Bereitstellung von IT-Ressourcen, wie Rechenkapazitäten, Speicher und Kommunikationsnetzen, sowie grundlegender Dienste für alle IT-Anwendungen. Dazu gehören Sicherheits- und Betriebsfunktionen, Online-Speicherdienste u. v. m. Dabei sollte berücksichtigt werden, dass die Kunden Anforderungen moderner IT-Anwendungen, beispielweise entsprechend dem Reaktiven Manifest (»Antwortbereit, widerstandsfähig und elastisch«), effektiv umsetzen können.

IT-Ressourcen sollten technisch vollständig virtualisiert werden, um die physischen Kapazitäten effizient auslasten zu können. Für die Bereitstellung von virtuellen Rechenkapazitäten sind entsprechende Technologien wie virtuelle Maschinen (IaaS), Container (CaaS) und Functions (FaaS) notwendig. Dabei sind offene Standards (wie Open Container Initiative (OCI) und Kubernetes) und offene Schnittstellen (beispielsweise zur automatischen Bereitstellung von Speicher) zu bevorzugen, um einen Vendor Lock-in zu vermeiden. IaaS, Caas und FaaS sind bei der Entwicklung öffentlicher IKT-Strategien und -Empfehlungen mitzudenken.

Die Deployment-Umgebung sollte ferner um eine offene, flexible Lösung zur medienbruchfreien Bereitstellung der IT-Anwendungen ergänzt werden (beispielsweise auf Basis des freien, verteilten Versionsverwaltungssystems Git), um kontinuierliche Deployment-Prozesse (beispielsweise nach dem GitOps-Prinzip) zu realisieren.

Die Modernisierung der IT-Infrastruktur des IT-Dienstleisters (Aufbau und Weiterentwicklung) bedarf eines initialen Invests.

Standardisierte Funktionalitäten durch IT-Dienstleister bedarfsgetrieben und zeitnah zur Verfügung stellen.

Statt wie bisher Ressourcen und Funktionalitäten kunden- respektive projektspezifisch und auftragsbasiert in entsprechenden Beschaffungszeiträumen bereitzustellen, sollten grundlegende »Produkte« im Rahmen eines vorausschauend ermittelten Gesamtbedarfes jederzeit »per Knopfdruck« verfügbar und abrufbar sein. Standardmäßig benötigte Ressourcen, wie Rechenkapazitäten, Speicher und Kommunikationsnetze, können dann in Standardgrößen (S, M, L, XL …) vorkonfektioniert durch den Kunden bzw. durch die/en Systempfleger:in im vertraglich vereinbarten Umfang direkt abgerufen werden. So kann der Kunde aktuell benötigte und neue Ressourcen im Rahmen der vertraglich vereinbarten Kontingente in einem Selbstbedienungsportal, also einem »Shop«, selbstständig aktivieren.

Sowohl der Umfang an Ressourcen als auch die vom Kunden für die IT-Anwendungen benötigten grundlegenden Dienste und Funktionen werden durch den IT-Dienstleister regelmäßig bedarfsorientiert ermittelt und fortgeschrieben, um jederzeit genug Ressourcen als Reserve vorzuhalten. Konsequenterweise werden auch die laufenden Kosten für die Ressourcen nach dem Prinzip »Pay-as-you-go« anteilig umgelegt, d. h. der Kunde zahlt nur für genutzte Ressourcen und Dienste. Dabei sind natürlich auch gemischte Abrechnungsmodelle denkbar, d. h. ein fixer Anteil und ein dynamischer Anteil entsprechend der tatsächlichen Nutzung. Für die öffentliche Verwaltung (wie auch für die Wirtschaft) geht damit die Herausforderung einher, auch entsprechend angepasste haushälterische Lösungen zu schaffen.

Nutzung von gemeinsamen, kooperativen Multi-Cloud-Lösungen durch die IT-Dienstleister.

Wesentliche Eigenschaften von Cloud-basierten IT-Anwendungen sind die Skalierbarkeit bzw. deren Elastizität bei wechselndem Lastverhalten sowie deren Verfügbarkeit (Ausfallsicherheit durch Redundanzen). Dazu sollten dahinterliegende Prozesse bzw. Dienste nicht nur mehrfach instanziiert, sondern auch auf redundanten Systemen ausgeführt werden. Um Ausfälle einzelner Standorte zu kompensieren, sollten die IT-Anwendungen je nach Schutzbedarf sowohl auf mehreren physischen Rechenzentren (bspw. innerhalb einer Gebietskörperschaft, Availability Zone) als auch idealerweise auf mehreren weit entfernten

CLOUD-ANWENDUNGEN SIND OHNE AUTOMATISIERUNG NICHT BETREIBBAR.

Standorten (Regions) verteilt ablaufen. Diese Risiko- und Lastverteilung von IT-Anwendungen erhöht die Resilienz und Leistungsfähigkeit der Anwendungen und damit die Souveränität und Handlungsfähigkeit des Staates.

Insbesondere die Verteilung von IT-Anwendungen auf mehrere Regionen bedeutet, dass mehrere unabhängige IT-Dienstleister dies nur gemeinsam realisieren können. Entsprechend ist es notwendig, dass diese kooperierenden IT-Dienstleister eine kompatible technische Plattform nutzen, um einerseits die Daten der IT-Anwendungen verteilt und redundant vorhalten und um andererseits das Ausführen der IT-Anwendungen und ihrer Rechenlasten jederzeit unterbrechungsfrei zwischen den Regionen verlagern zu können. Die Entwicklung solcher interoperabler Plattformen wird beispielsweise aktuell im Rahmen der Europäischen Datenplattform und im Projekt GAIA-X (Sovereign Cloud Stack, https://scs.community) des BMWI vorangetrieben.

Bestehende und zukünftige Standards und Schnittstellen zur Nutzung und Bereitstellung von Cloud-Ressourcen sollten unterstützt werden.

Abbildung verwaltungstypischer Prozesse beim Deployment.

Die Installation und die Aktualisierung von IT-Anwendungen werden bisher meist nur in Bezug auf eine spezifische Umgebung betrachtet, beispielsweise nur die Entwicklungs- oder nur die Produktionsumgebung. Zweckmäßiger für die Verwaltung ist ein mehrstufiges Verfahren. Als erfolgreiche Vorgehensweise hat sich folgendes mehrstufiges Verfahren (Staging) etabliert: Entwicklungsumgebung (Entwickler:in) ► Prüfumgebung (Betreiber, optional) ► Abnahmeumgebung (Betreiber) ► Schulungsumgebung (Betreiber) ► Produktionsumgebung (Betreiber) (vgl. Abb. 6).

Daraus folgt unmittelbar, dass der IT-Dienstleister mehrere, gleichartige Cloud-Umgebungen (Cluster) parallel in verschiedenen Sicherheitszonen bereitstellen sollte. Ferner sollten automatisierte Prozesse realisiert werden, die eine sichere, medienbruchfreie Übernahme der von den Entwickler:innen (über das Internet) gelieferten Software ermöglichen (Continuous Delivery). Eine automatisierte Übernahme der IT-Anwendung in die verschiedenen oben genannten Umgebungen kann dann schrittweise erfolgen (Continuous Deployment). Die Freigabe für jeden Schritt erfolgt dabei manuell durch die/den Verantwortliche:n für die IT-Anwendung.

Deployment und Betriebsführung eines IT-Fachverfahrens durch selbstständige Kunden.

Das bisher übliche manuelle Deployment mittels Change Requests bzw. Tickets und Betriebshandbuch ist bei verteilten IT-Anwendungen zu aufwändig, fehlerträchtig und vor allem zu langsam. Im Zeitalter des agilen Vorgehens sollte auch das Deployment häufiger und zeitnah erfolgen können. Dafür sollte nicht nur der Deployment-Prozess durchgängig automatisiert sein, sondern auch die Steuerung des Deployments direkt durch den Kunden selbstständig erfolgen können, ohne dass Mitarbeiter:innen vom Systembetrieb des IT-Dienstleisters eingreifen müssen. Der Kunde benötigt eine Selbstbedienungsoberfläche (»Shop«), um benötigte Ressourcen zu verwalten. Auch erlaubt sie dem Kunden den Zugang zu Werkzeugen für seinen IT-Anwendungsbetrieb, bspw. für das Monitoring der genutzten Ressourcen oder die Nutzung von Betriebsprotokollen der IT-Anwendung. Auch sollten Programmierschnittstellen (APIs) zur Verfügung stehen, um Prozesse der Deployment-Umgebung automatisiert steuern und überwachen zu können.

IAAS, CAAS UND SAAS SIND
OHNE OAAS SCHWER DENKBAR.

IT-Dienstleister brauchen eigene Entwicklungsteams für die Weiterentwicklung der Automatisierung.

Der enorme Erfolg der Unternehmen der Internetökonomie beruht darauf, dass durch die Automatisierung von Routineaufgaben Angebote nicht nur kostengünstiger werden, sondern vor allem auch neue und höherwertige Dienstleistungen angeboten werden können. Für einen IT-Dienstleister heißt dies, dass einerseits bisher gängige Administrationstätigkeiten durch Programme ersetzt werden und andererseits Kunden in die Lage versetzt werden, anwendungsspezifische Administrationsaufgaben selbst (automatisiert) zu realisieren (DevOps). Für die Automatisierung der Infrastruktur (inkl. Selbstbedienungsportal, API usw.) benötigt ein IT-Dienstleister selbst Softwareentwickler:innen bzw. die vorhandenen Administrator:innen müssen lernen, wie sie ihre bisher manuell durchgeführten Tätigkeiten durch Skripte und Programme um- respektive ersetzen können.

Es sollte sichergestellt sein, dass die Prozesse für die Kernaufgaben des IT-Dienstleisters bei Bedarf jederzeit durch eigenes Personal angepasst und kontinuierlich betrieben werden können. Diese Entwicklungstätigkeiten sollten nicht vollständig »outsourced« werden, um nicht die Kontrolle über die eigenen Kernprozesse zu verlieren. Auch sollte ein IT-Dienstleister die interne Organisation an die »Produktorientierung« anpassen (beispielsweise durch agile Teams).

Um die Mitarbeiter:innen mitzunehmen, muss der Umstieg disruptiv erfolgen – ab heute.

Die Umstellung auf die Cloud, insbesondere Container-as-a-Service (CaaS) bzw. Function-as-a-Service (FaaS) stellt für IT-Dienstleister eine sehr große Herausforderung dar. Es geht nicht nur um Technik, sondern um Menschen. Vor allem geht es dabei auch um ein neues Selbstverständnis (»weg von Turnschuh-Administration hin zur automatisierten Dienstleistung«) und eine damit einhergehende veränderte Kultur (»wir sind Entwickler:innen unserer Ops-Lösung«). Ein derartiger Sprung ist nicht mehr nebenbei und schleichend zu bewältigen, sondern sollte mit dem Aufbau neuer Cloud-Strukturen disruptiv erfolgen.

So sollte man die »neue Cloud-Welt« (CaaS und IaaS) als neue Dienstleistung mit entsprechenden Organisationstrukturen aufbauen und vollautomatisiert betreiben. Gleichzeitig sollte man die bisherigen Lösungen weiterhin betreiben, aber auslaufen lassen und schrittweise migrieren. Um die Umstellungsprozesse zum Erfolg zu führen, ist es wichtig, die Mitarbeitenden mitzunehmen und nicht zu überfordern. Vor allem sollten die Menschen dabei unterstützt werden, diesen Modernisierungssprung mit seinen vielen Veränderungen zu bewältigen – beispielsweise durch begleitende Weiterqualifizierungen und intensive Coachings zur agilen Vorgehensweise. Um aber den Umsetzungsdruck nicht noch weiter und unnötig zu erhöhen, empfiehlt es sich, frühzeitig, d. h. jetzt und heute, mit dem Umstieg zu beginnen. Ein zeitnaher Umstieg kann auch helfen, motivierte Mitarbeiter:innen zu begeistern und zu binden. Begeisterte Mitarbeiter:innen sind meist auch diejenigen, die dann ihre Kolleg:innen später durch den Veränderungsprozess mitnehmen können.

Die digitale Souveränität des Staates sowie die Hoheit über seine Daten und deren Verarbeitung muss garantiert werden

Die in diesen Handlungsempfehlungen geschilderte Weiterentwicklung – nicht nur bei IT-Dienstleistern, sondern des gesamten Prozesses von der Entwicklung bis zur Bereitstellung von modernen IT-Anwendungen – kann insgesamt zur digitalen Souveränität des Staates beitragen. Viele der genannten Maßnahmen erfüllen nicht nur einen unmittelbaren Zweck, sondern wirken auch in einem übergreifenden, strategischen Rahmen zusammen. Offene Schnittstellen verhindern nicht nur Vendor Lock-in für die IT-Anwendungen, sie erweitern auch die Handlungsoptionen des Staates und können zu Innovation und Wettbewerbsfähigkeit in der Wirtschaft beitragen. Auch die

Abbildung 7: Cloud in Selbstbedienung durch die öffentliche Verwaltung

Risiko- und Lastverteilung von IT-Anwendungen erhöht die Handlungsfähigkeit des Staates, beispielsweise bei der Bewältigung lokaler Ausfälle, ob aufgrund technischer Probleme oder als Folge von Angriffen auf die IT.

Bei der Verarbeitung von Daten muss sichergestellt sein, dass diese für festgelegte, eindeutige und legitime Zwecke sowie in rechtmäßiger und nachvollziehbarer Weise verarbeitet werden. Insbesondere dürfen die Daten nicht in den Besitz von unberechtigten Dritten gelangen (Vertraulichkeit) oder durch diese manipuliert werden (Integrität). Trotz Virtualisierung der Ressourcen sollte daher angestrebt werden, dass der Digitale Raum [2], in dem Daten verarbeitet, gespeichert und übermittelt werden, sich physisch im eigenen Hoheitsgebiet und unter der eigenen Hoheit befindet [1]. Erreichen lässt sich dies dadurch, dass zu schützende Daten auf der digitalen Infrastruktur von nationalen öffentlichen IT-Dienstleistern innerhalb des Hoheitsgebietes verarbeitet, gespeichert und übermittelt werden. Je nach Ergebnis einer Risikoanalyse kann der Digitale Raum auch die EU oder sogar andere Weltregionen umfassen.

Aus wirtschaftlichen Gründen, aufgrund der technischen Möglichkeiten sowie um kurzfristig zusätzliche IT-Ressourcen zur Verfügung zu haben, sollten IT-Anwendungen auch auf Systemen von Dritten wie kommerziellen IT-Dienstleistern ausgeführt werden, wenn das ermittelte Schutzniveau dies erlaubt. In solch einem Fall sollte die IT-Anwendung aber jederzeit auch kurzfristig auf alternative Systeme verlagert werden können, um bei Problemen die Hoheit über die IT-Anwendung wieder herzustellen zu können.

LITERATUR

[1] **Jörg Schieb:** Wenn der US-Präsident die Cloud ausknipst, https://blog.wdr.de/digitalistan/wenn-der-us-praesident-die-cloud-ausknipst/, 14.10.2019.

[2] **Utz Schliesky et al.:** Digitale Räume als Teil der Daseinsvorsorge, Lorenz-von-Stein-Institut, Kiel, 2018.

[3] **Jonas Bonér, Dave Farley, Roland Kuhn und Martin Thompson:** Das Reaktive Manifest, https://www.reactivemanifesto.org/de, 16.09.2014 (v2.0).

[4] **Michael Stemmer et al.:** Cloud Computing. In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, https://www.oeffentliche-it.de/-/cloud-computing, 2014.

[5] **Peter H. Deussen et al.:** Cloud-Fahrplan öffentliche Verwaltung, Hg.: Kompetenzzentrum Öffentliche IT, https://www.oeffentliche-it.de/documents/10181/14412/Cloud-Fahrplan+%C3%B6ffentliche+Verwaltung, 2014.

[6] **Jan Gottschick et al.:** Microservices. In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, https://www.oeffentliche-it.de/-/microservices, 2019.

[7] H.R.4943 – CLOUD Act – 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/4943.

[8] **innoQ:** Self-Contained Systems – Assembling Software from Independent Systems, https://scs-architecture.org.

[9] **Eric Evans:** Domain-Driven Design: Tackling Complexity in the Heart of Software, Addison-Wesley, 2004.

[10] **The Linux Foundation:** Production-Grade Container Orchestration – Automated container deployment, scaling, and management, https://kubernetes.io.

[11] **Chris Riley:** Meet Infrastructure as Code, https://devops.com/meet-infrastructure-code, DevOps.com, 2014.

[12] **Open Container Initiative:** An open governance structure for the express purpose of creating open industry standards around container formats and runtimes, https://www.opencontainers.org.

[13] **Axelos:** ITIL Foundation, ITIL 4 edition, https://www.tso-shop.co.uk/Business-and-Management/AXELOS-Global-Best-Practice/ITIL-4, 2020.

[14] **P. Mell und T. Grance:** The NIST Definition of Cloud – Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, 2011.

[15] **A. Brandolini:** Introducing EventStorming: An act of Deliberate Collective Learning, Leanpub, 2018.

[16] **Bundesamt für Sicherheit in der Informationstechnik (BSI):** IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

CLOUD-LEXIKON

Abkürzungen

API – Application Programming Interface ► Programmierschnittstelle

CaaS ► Container-as-a-Service

CI/CD ► Continuous Integration, Continuous Delivery, Continuous Deployment

DDD ► Domain-Driven Design

Dev – Developer ► Softwareentwickler:in

DSGVO ► Datenschutzgrundverordnung

FaaS – Function-as-a-Service ► Serverless Functions

IaaS ► Infrastructure-as-a-Service

IaC ► Infrastructure-as-Code

K8s ► Kubernetes

OCI ► Open Container Initiative

Ops – Operator ► Systemadministrator:in

SoA ► Service-oriented Architecture

VCS – Version Control System ► Versionsverwaltungssystem

Bereitstellung (von IT-Ressourcen) ► Provisioning

Bereitstellungsprozess (von IT-Anwendungen) ► Deployment

Betreiber (der IT-Ressourcen) ► IT-Dienstleister

Betriebshandbuch
Installations- und Betriebsanleitung, mit deren Hilfe die/der Systemadministrator:in in der Lage ist, eine IT-Anwendung auf den technischen Systemen zu betreiben (»zum Laufen bringen«).

Change Request
Eine Änderungsanforderung bzgl. der Software bei der/dem Softwareentwickler:in oder bzgl. der Systemumgebung bzw. der Betriebsparameter beim IT-Dienstleister. [13]

Cloud
Cloud-Computing ist ein Modell für einen allgegenwärtigen, bequemen, bedarfsorientierten Netzzugang zu anpassbaren IT-Ressourcen (beispielsweise Netzwerken, Servern, Speicher, IT-Anwendungen und Diensten), der mit minimalem Verwaltungsaufwand oder durch einen IT-Dienstleister schnell bereitgestellt und freigegeben werden kann. [14]

Cluster ► Container-Cluster

Container
Virtualisierungstechnik, um eine IT-Anwendung in einer eigenen Laufzeit- und Systemumgebung auszuführen. Die Container-Virtualisierung erlaubt es, mehrere Container auf einem Host gleichzeitig und damit wirtschaftlich vorteilhaft auszuführen. Die Container teilen sich dazu die IT-Ressourcen des Hosts. Container können effektiv und effizient voneinander abgeschottet werden. Container-Images eignen sich auch als bevorzugtes Medium für die Verteilung vorkonfigurierter Software.

Container-Cluster
Ein Container-Cluster fasst mehrere physische/virtuelle Rechner zusammen und sieht nach außen wie ein geschlossenes System aus. In dem Container-Cluster werden dann die Container möglichst gleichmäßig auf die verschiedenen Rechner verteilt, um die Rechen- und Speicherkapazitäten der Rechner optimal auszunutzen. Container können auch redundant verteilt und ausgeführt werden, um Ausfälle einzelner Rechner des Clusters (für die Nutzer:innen transparent) zu kompensieren.

BEIM DEVOPS-PRINZIP WIRD SCHON BEI DER ENTWICKLUNG DAS DEPLOYMENT BERÜCKSICHTIGT.

Container-Image
Ein Container-Image ist ein virtuelles Medium, um ein komplettes System mit allen benötigten Dateien (Daten und Programme) zu verteilen, das als Container gestartet und ausgeführt werden kann. Ein Container wird generell abgeschottet und bietet seine Funktionalität über eine explizit freigegebene Netzwerkschnittstelle (API) an.

Container-Orchestrierung
Die Container-Orchestrierung verwaltet die Ressourcen eines Container-Clusters (siehe auch Kubernetes). Die Ressourcen umfassen nicht nur die Container des Container-Clusters, sondern auch weitere Artefakte, wie persistente Speicher oder abstrakte Hilfsmittel wie Dienstdefinitionen.

Container-as-a-Service
Bei Container-as-a-Service (CaaS) offeriert und betreibt der IT-Dienstleister nicht nur einzelne (virtuelle) Rechner wie beim Infrastructure-as-a-Service (IaaS), sondern Container-Cluster inklusive der Container-Orchestrierung (beispielsweise Kubernetes).

Container-Registry
Die Container-Registry ist ein Infrastruktur-Dienst, der zentral Container-Images bereitstellt. Die Container-Images werden beim Start einer Cloud-Anwendung aus der Container-Registry geladen und als Container in einem Cluster ausgeführt.

Continuous Delivery
Teilprozess eines CI/CD-Prozesses, der die fertigen Images, Binaries (übersetzte Dateien), Quellcode und Dokumentation an den Auftraggeber medienbruchfrei übergibt, bspw. indem er diese Artefakte in einem Versionsverwaltungssystem (z. B. Git) des Auftraggebers ablegt.

Continuous Deployment
Teilprozess eines CI/CD-Prozesses, der mittels der an den Auftraggeber übergebenen Artefakte die Container der Cloud-Anwendung im Container-Cluster startet.

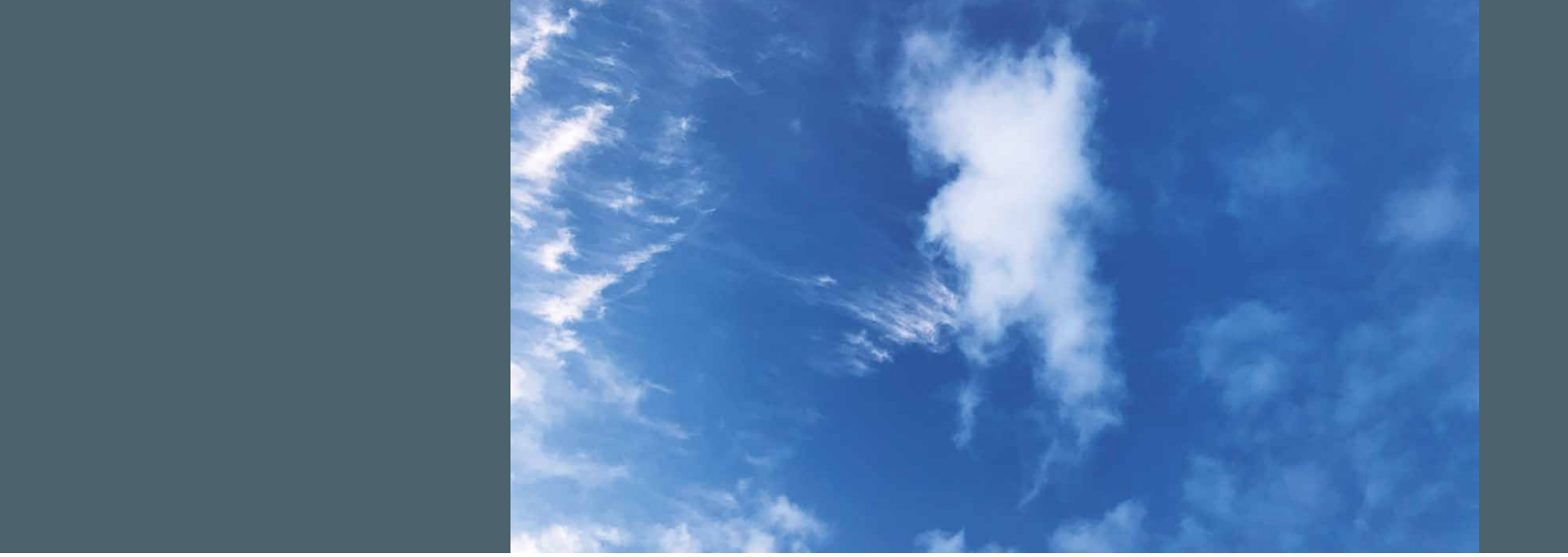
Continuous Integration
Teilprozess eines CI/CD-Prozesses, der aus dem Quellcode für die Cloud-Anwendung die Binaries für das Deployment erzeugt. Zusätzlich beinhaltet der Teilprozess abnahmerelevante Maßnahmen (QS), wie beispielsweise das Ausführen von automatischen Abnahmetests der Software oder die automatische Überprüfung eines erfolgreichen Deployments.

Deployment
Dies umfasst alle notwendigen Tätigkeiten, um eine Software, die ein:e Softwareentwickler:in an den Auftraggeber (beispielsweise die Verwaltung) ausgeliefert hat, auf den IT-Systemen beim IT-Dienstleister bereitzustellen (d. h. zu installieren bzw. zu aktualisieren). In der Praxis ist damit aber auch organisatorisch ein verbindlicher Prozess verbunden, der Testen, Abnahme, Schulung, Produktion und Fehlersuche bei Problemen berücksichtigt. Dazu muss die gelieferte Software auf unterschiedlichen Systemen parallel bereitgestellt werden.

Deployment-Umgebung
Die Deployment-Umgebung beschreibt die spezifische (und in der Regel eingeschränkte) Systemumgebung beim IT-Dienstleister, in der die von den Softwareentwickler:innen gelieferte Software lauffähig sein muss.

DevOps-Prinzip
Beim DevOps-Prinzip werden schon bei der Entwicklung der Software die Prozesse des Deployments stark berücksichtigt. Installation und Wartung der Software sollten weitestgehend automatisiert sein, sodass für Konfiguration, Deployment und Betrieb kein Eingreifen des Operators (Ops) notwendig ist. Entsprechend ist im Entwicklungsprozess eine starke Einbindung von Systemadministrator:innen und deren Wissen notwendig.

Dienstleistungsvereinbarung
Eine Dienstleistungsvereinbarung beschreibt die Rechte und Pflichten des IT-Dienstleisters. Diese beinhalten nicht nur Tätigkeitsumfang, Prozesse, Sicherheitsanforderungen u. v. m., son-



dern auch einzuhaltende Kennwerte, wie beispielsweise die Verfügbarkeit oder Antwort- und Verzögerungszeiten für Dienstaufrufe.

Digitaler Raum

Ein Digitaler Raum umfasst alle physischen und virtuellen IT-Ressourcen und Kommunikationsverbindungen, die eine IT-Anwendung direkt oder indirekt nutzt. Der geografische Raum, über den sich ein Digitaler Raum erstreckt, ist prinzipiell durch die geografischen Standorte aller betroffenen IT-Ressourcen sowie den Verlauf aller physischen Netzkabel bestimmt. (Siehe auch ► Hoheitsgebiet)

Domain-Driven Design

Das Domain-Driven Design (DDD) [15] ist eine Analysemethode, um eine komplexe IT-Anwendung in klar abgegrenzte, funktionale/fachliche Domänen zu zerlegen. Jede Domäne hat einen abgegrenzten Kontext (Bounded Context), der Entitäten und Aggregate kapselt sowie eine eindeutige Begriffswelt (ubiquitäre Sprache) umfasst. Die bei der Analyse entstehenden Domänen sind potenzielle Kandidaten für Dienste (Microservices) der IT-Anwendung. Die Grenze einer Domäne und die auszutauschenden Datenobjekte zwischen Domänen sind die Basis für die Schnittstelle eines Dienstes.

Function-as-a-Service ► Serverless Functions

Hoheitsgebiet

»Die rechtliche Grundlage für die räumliche Gliederung der Verwaltung ist das sogenannte Territorialprinzip. Es besagt, dass der Wirkungskreis eines Organs nach örtlichen Grenzen abgesteckt wird; für das Handeln der Behörde bzw. des Organs wird mithin auf ein bestimmtes Territorium, insbesondere auf einen bestimmten Teil des Staatgebietes abgestellt.« [2]

Hybrid-Cloud

Normalerweise nutzt man für eine IT-Anwendung nur einen Cloud-Betreiber. Hybrid-Cloud bezeichnet Mischformen aus eigenen IT-Ressourcen (traditionelles Rechenzentrum vor Ort oder eine exklusive, zugangsbeschränkte Private-Cloud beispielsweise in einem zentralen Rechenzentrum) und der Nutzung öffentlich zugänglicher Cloud-Angebote. Die Private-Cloud wird vor allem mit Kontrollmöglichkeiten und hohem Schutzniveau verbunden, die Public-Cloud steht zuvorderst für Wirtschaftlichkeit und Flexibilität. Über die Nutzung verschiedener Cloud-Angebote lässt sich die Leistung der IT-Anwendungen verbessern, siehe auch ► Multi-Cloud.

Infrastructure-as-a-Service

Dies ist das Cloud-Angebot eines Cloud-Betreibers, bei dem physische und virtuelle Maschinen sowie Speicher inklusive der notwendigen Infrastruktur und Kommunikationsverbindungen temporär vermietet werden. Durch Automatisierung und Selbstbedienung können Kunden sehr flexibel und kosteneffizient benötigte IT-Ressourcen nutzen und kurzfristig skalieren, ohne selbst in eigene IT-Hardware zu investieren und diese zu betreiben.

Infrastructure-as-Code

Herkömmlich werden alle benötigten IT-Ressourcen inklusive Netzwerk durch die Systemadministrator:innen installiert und konfiguriert. Bei Infrastructure-as-Code deklarieren die Entwickler:innen der Software (Developer) und/oder die Systemadministrator:innen (Operator) die Installation und Konfiguration von IT-Ressourcen und Netz für die konkrete IT-Anwendung als ausführbare Spezifikation oder Programmcode, sodass diese Infrastruktur automatisch durch die Systemumgebung eingerichtet werden kann.

IT-Anwendung

Eine IT-Anwendung implementiert Funktionen und Geschäftsprozesse durch Software und automatisiert bzw. digitalisiert damit einen Teil der Tätigkeiten von Anwendern.

IT-Dienstleister

Ein IT-Dienstleister stellt IT-Ressourcen, wie Rechenkapazitäten,

KUBERNETES IST DAS
»BETRIEBSSYSTEM DER CLOUD«.

Speicher und Kommunikationsverbindungen, physisch oder auch virtualisiert bereit und betreibt diese. Kunden können diese IT-Ressourcen mieten und darauf ihre IT-Anwendungen betreiben bzw. durch den IT-Dienstleister betreiben lassen.

IT-Fachverfahren

Ein IT-Fachverfahren implementiert bzw. digitalisiert einen oder mehrere Geschäftsprozesse einer Fachdomäne. (Siehe auch ► IT-Anwendung)

IT-Ressource

Als IT-Ressource werden hier zunächst physische Ressourcen wie Rechner, Speicher und Kommunikationsverbindungen bezeichnet, die zur Ausführung von IT-Anwendungen benötigt werden.

Kubernetes

Kubernetes (https://kubernetes.io/) ist als Industriestandard der De-facto-Standard zur Orchestrierung von Containern in einem Container-Cluster. Der Standard beschreibt, wie eine IT-Anwendung mit ihren zugehörigen IT-Ressourcen zu installieren und zu konfigurieren ist.

Microservices

Ein Microservice ist eine leichtgewichtige Umsetzung eines Dienstes im Sinne der Service-oriented Architecture (SoA) und wird in der Regel von einem Entwicklungsteam verantwortet. Der Funktionsumfang eines Microservices kann mithilfe von Analysemethoden wie dem Domain-Driven Design [9] oder Event-Storming [15] ermittelt werden.

Multi-Cloud

Normalerweise betreibt man eine Cloud-Lösung nur bei einem Cloud-Betreiber. Um beispielsweise die Ausfallsicherheit und Skalierbarkeit zu erhöhen oder kurze Latenzzeiten zu gewährleisten, wird diese auf IT-Ressourcen in verschiedenen Standorten und Regionen verteilt. Ist diese Verteilung nicht durch einen einzigen Cloud-Anbieter zu realisieren, kann die Cloud-Anwendung auch auf mehrere Cluster von verschiedenen Cloud-Anbietern (IT-Dienstleistern) mit gleicher Technologie und gleichem Funktionsumfang verteilt werden. Es werden aber auch spezielle Cloud-Angebote offeriert, bei denen das Cluster anstelle eines Universalprozessors spezielle Rechenwerke wie Grafikbeschleuniger und/oder spezielle Dienste anbietet, bspw. KI-Funktionen zum maschinellen Lernen oder zukünftig Quantencomputing. Es kann also für eine Cloud-Anwendung zweckmäßig sein, gleichzeitig mehrere Clouds zu nutzen, wobei einige Cluster spezielle Funktionalitäten oder Qualitätsmerkmale anbieten, beispielsweise eine hohe Performanz.

Open Container Initiative

Die Open Container Initiative (https://www.opencontainers.org) standardisiert sowohl die Erstellung von Container-Images (image-spec) als auch die Laufzeitumgebung zum Ausführen von Containern (runtime-spec).

Operator ► siehe Systemadministrator:in

Pay-as-you-go

Eine Cloud kann man nicht nur vor Ort auf eigenen, physischen IT-Ressourcen realisieren (on-premise), sondern auch auf (virtualisierten) IT-Ressourcen von Dritten (IT-Dienstleistern) und diese über das Internet oder private Netze nutzen. Wenn die Bereitstellung von IT-Ressourcen beim IT-Dienstleister flexibel und insbesondere in Selbstbedienung erfolgt, können die Nutzer einer Cloud die Nutzung der IT-Ressourcen kurzfristig (automatisiert) anpassen. Bei Pay-as-you-go bezahlt der Nutzer nicht die über einen vertraglich vereinbarten Zeitraum maximal benötigten IT-Ressourcen, sondern nur die IT-Ressourcen, die innerhalb einer Zeiteinheit (Abrechnungseinheit) tatsächlich genutzt werden.

Portal

Ein webbasiertes Portal bietet Nutzer:innen einen transparenten und zentralen Zugangspunkt zu mehreren IT-Anwendungen. In der Regel ist nicht erkennbar, dass das Portal unterschiedliche IT-Anwendungen zusammenfasst, da Nutzerführung

und Aussehen einheitlich gestaltet werden. Gemeinsame Funktionen verschiedener IT-Anwendungen werden einmalig und einheitlich realisiert, wie beispielsweise das An- und Abmelden von Nutzer:innen.

Programmierschnittstelle

IT-Anwendungen werden zur Reduzierung der Komplexität in kleinere Einheiten zerlegt, bspw. in Microservices (siehe dort). Diese Dienste haben eine klar abgegrenzte Funktionalität (siehe Domain-Driven Design). Microservices nutzen die Funktionalität von anderen Diensten bzw. tauschen mit diesen Daten und Ereignisse aus. Dazu bieten sie (einen Teil) ihrer Funktionalität mittels Kommunikationsendpunkten über Programmierschnittstellen an, damit diese von anderen Komponenten genutzt werden können. Eine Programmierschnittstelle muss formal eindeutig spezifiziert sein, um eine interoperable Kommunikation gewährleisten zu können.

Provisioning

Die Bereitstellung von IT-Ressourcen für eine IT-Anwendung durch den IT-Dienstleister.

Reactive System

Entsprechend dem Reaktiven Manifest [3] sind Reactive Systems antwortbereit (responsive), widerstandsfähig (resilient), elastisch (elastic) und nachrichtenorientiert (message-driven). Diese Eigenschaften sind beispielsweise von populären Onlineangeboten bekannt.

Schutzbedarf

Der Schutzbedarf von Zielobjekten (Daten, IT-Systemen usw.) entsprechend IT-Grundschutz [16] legt anhand der Gefährdungen die zu treffenden Sicherheitsmaßnahmen fest.

Schutzniveau

Das angemessene Schutzniveau für personenbezogene Daten gemäß DSGVO legt fest, dass die/der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen hat, um einen ausreichenden Schutz der Daten zu gewährleisten und die Risiken für die Rechte der Betroffenen einzudämmen (siehe auch Schutzbedarf).

Self-Contained Systems

Self-Contained Systems (SCS) [8] sind in sich vollständige IT-Anwendungen, die eine klar umgrenzte Fachlichkeit bzw. Domäne umsetzen (siehe auch Domain-Driven Design). Das Self-Contained System umfasst alle Ebenen einer IT-Anwendung, d. h. die Benutzungsoberfläche (Frontend), ein oder mehrere Microservices mit der Geschäftslogik und die persistente Speicherung von Daten. Ein Self-Contained System wird durch ein Entwicklungsteam verantwortet.

Serverless Functions

Serverless Functions sind eine Weiterentwicklung von Cloud-Containern und ermöglichen Softwareentwicklern, zustandslose Cloud-Funktionen sehr einfach zu implementieren und bereitzustellen. Die Implementierung von Serverless Functions (Functions-as-a-Service, FaaS) ist auf die Schnittstelle und Funktion reduziert. Die Widerstandsfähigkeit und Elastizität der Serverless Functions wird durch die Orchestrierung sichergestellt.

Services Mesh

Die Bereitstellung notwendiger Microservices bzw. die Dekomposition von IT-Anwendungen als Self-Contained Systems führt schnell zu vielen Komponenten, die sicher, zuverlässig und effizient miteinander sowie extern kommunizieren müssen. Da eine manuelle Konfiguration der Kommunikationsverbindungen durch die Vielzahl der Verbindungen und durch das häufige Deployment neuer Versionen im Rahmen der agilen Entwicklung von IT-Anwendungen nicht praktikabel ist, werden die Kommunikationsverbindungen automatisch durch das Service Mesh (Orchestrierung des Kommunikationsnetzes) eingerichtet und verwaltet. Diese Automatisierung vereinfacht sowohl die Entwicklung von Microservices als auch deren sicheren und zuverlässigen Betrieb.

DER DEPLOYMENT-PROZESS STELLT SICHER, DASS SOWOHL TECHNISCHE ALS AUCH ORGANISATORISCHE RAHMENBEDINGUNGEN EINGEHALTEN WERDEN.

Service-oriented Architecture

IT-Anwendungen können sehr komplex sein und viele Tausende bis Millionen Zeilen von Programmcode umfassen. Daher gilt es, diese Monolithen in überschaubar große Komponenten mit abgegrenztem Funktionsumfang zu zerlegen. Um eine enge Kopplung und damit Abhängigkeit zwischen den Komponenten zu vermeiden, werden die Komponenten im Rahmen der Service-oriented Architecture (SoA) als Dienste gekapselt und mit Kommunikationsschnittstellen ausgestattet, um Daten zwischen Diensten austauschen zu können. Als Dienst gekapselte Funktionalitäten können in anderen Kontexten leicht wiederverwendet werden.

Skript

Skripte sind Programme, die einfach und schnell ohne Entwicklungsumgebung geschrieben werden können. Da sie nicht in Maschinencode o. Ä. übersetzt werden, werden sie vorab nicht zwingend auf syntaktische oder semantische Fehler überprüft. Skripte werden erst zur Laufzeit interpretiert und können daher zur Laufzeit häufiger zu solchen Fehlern führen.

Softwareentwickler:in

Softwareentwickler (Developer, Dev) bekommen die an eine IT-Anwendung gestellten Anforderungen und setzen diese in ausführbaren Programmcode um. Die fertig entwickelte Software wird dann vom Kunden nach entsprechender Prüfung abgenommen und durch eine:n Systemadministrator:in oder einen automatisierten Deployment-Prozess auf den Zielsystemen installiert.

Systemadministrator:in

Der/die Systemadministrator:in (Operator, Ops) installiert und pflegt IT-Anwendungen auf den Zielsystemen (IT-Ressourcen) und betreibt die IT-Ressourcen aus technischer Sicht.

Staging

Vom Softwareentwickler erstellte IT-Anwendungen werden nicht direkt in der Produktionsumgebung bereitgestellt. Stattdessen wird einem Deployment-Prozess gefolgt, bei dem die IT-Anwendung schrittweise (bspw. Test ► Abnahme ► Schulung ► Produktion) in verschiedenen Systemumgebungen (Stages) bereitgestellt wird.

Systemumgebung

IT-Anwendungen werden in einer Systemumgebung installiert und damit bereitgestellt. Die Systemumgebung besteht dabei nicht nur aus dem Betriebssystem, sondern umfasst auch die benötigten Bibliotheken (mit passendem Versionsstand), weitere Programme und Kommunikationsverbindungen zu anderen Diensten und nach extern.

(Trouble-)Ticket-System

Ein (Trouble-)Ticket-System dient zur Kommunikation zwischen Kunden und Auftragnehmer, bspw. dem IT-Dienstleister oder Softwarentwickler:innen. Ein Ticket kann sich auf eine Störungsmeldung (Fehler), aber auch auf einen Änderungswunsch beziehen. Tickets enthalten nicht nur die ausgetauschten (Offline-)Nachrichten von Kunde und Auftraggeber, sondern auch Meta-Informationen, beispielsweise um den Bearbeitungsstand/-ablauf dokumentieren und nachvollziehen zu können.

Versionsverwaltungssystem

Ein Versionsverwaltungssystem ist ein Repository (persistente Dateiablage), um Programmcode, Dokumentation u. A. im Rahmen der Softwareentwicklung organisationsintern ablegen zu können. Dabei kann die Historie einer Datei nachverfolgt werden, da jede veränderte Datei als eigene Version gespeichert wird. Ein Versionsverwaltungssystem (beim Kunden) kann auch zur offiziellen, medienbruchfreien Übergabe von Releases einer IT-Anwendung von der/dem Softwareentwickler:in an den Kunden/IT-Dienstleister verwendet werden, anstelle eines physischen Mediums (bspw. CD).

Virtuelle Maschine

Um die Rechen- und Speicherkapazitäten eines physischen Rechners besser auslasten zu können, können diese durch Virtualisierungstechnik mehreren virtuellen Maschinen zugeteilt werden.

KONTAKT

Jens Tiemann
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-948582-05-0

kre | 2102 (Fotos: pixabay, ÖFIT; Illustration: Martha Friedrich;
Icons für Infografik: fontawesome)