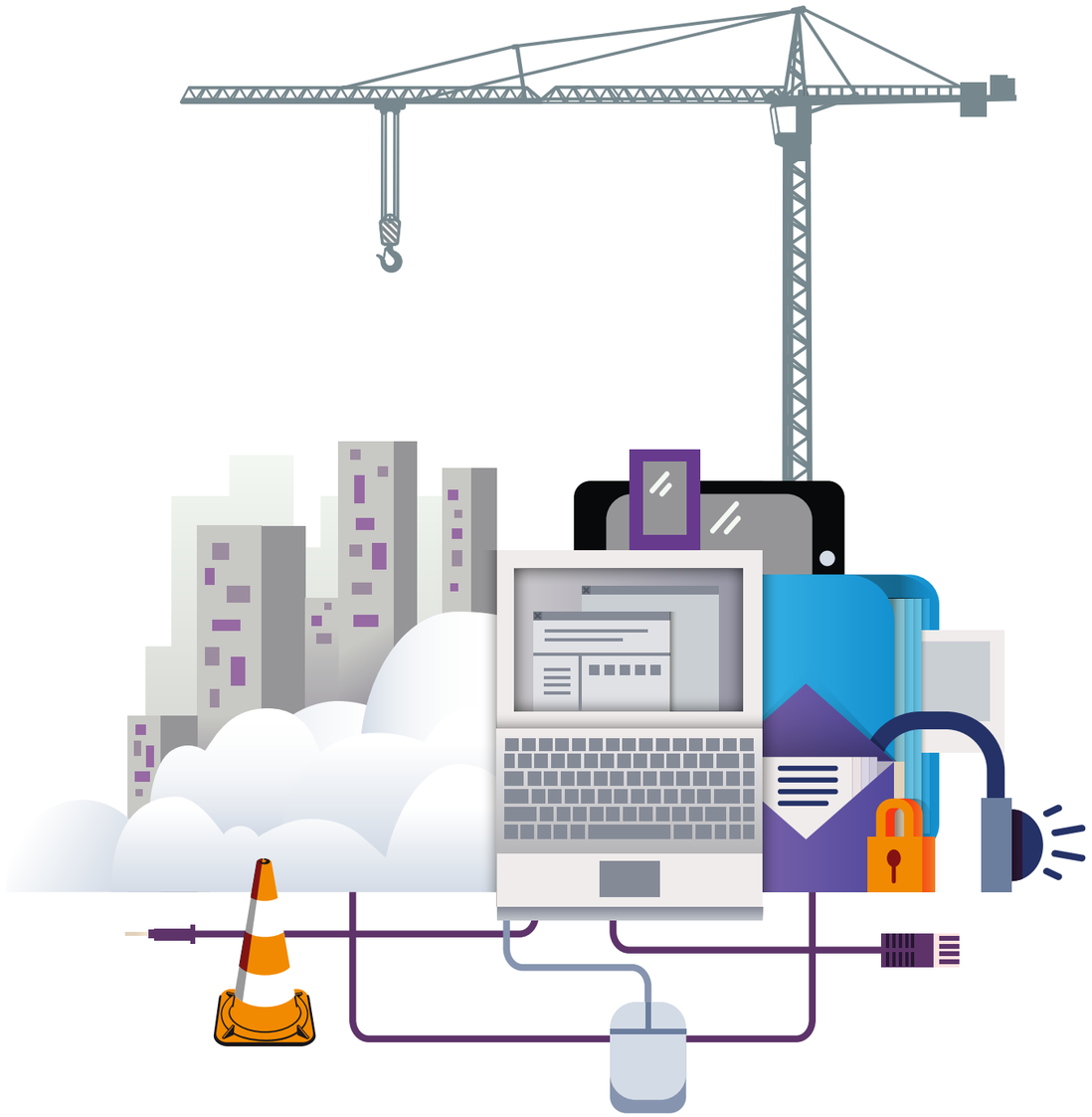
LÜNENDONK Magazin

Ausgabe 11/2023

Schwerpunkte
Cloud-Strategie
Best Practices
Cloud Security

Cloud Transformation –

Business und IT auf dem Weg in die Zukunft



Mario Zillmann

Partner
Lünendonk &
Hossenfelder

Vorab

Liebe Leserin, lieber Leser,

Die digitale Transformation braucht Power. Und die kommt immer häufiger aus der Cloud. Egal ob Rechenkapazitäten, Entwicklerplattformen, Cloud-native-Architekturen oder Software as a Service:

Immer mehr Unternehmen und auch der öffentliche Sektor forcieren ihre Investitionen in die IT-Modernisierung und in die Digitalisierung ihrer Prozesse und Geschäftsmodelle. Tatsächlich ist die Cloud längst kein reines IT-Thema mehr. Mittlerweile sind es immer häufiger die Fachbereiche, die die IT zu mehr Geschwindigkeit bei der Einführung von Cloud-Services drängen, um sich den sich rasant verändernden Kunden- und Marktanforderungen anzupassen. Ziele wie Agilität, Flexibilität und Skalierbarkeit von Geschäftsprozessen und digitalen Produkten stehen dabei oft im Fokus.

Laut Lünendonk-Research hat sich der überwiegende Teil der Unternehmen und Behörden im deutschsprachigen Raum auf den Weg in die Cloud-Transformation begeben. Immerhin gilt die Cloud als wesentliche Voraussetzung für die Digitalisierung von Geschäftsmodellen, für moderne Geschäftsprozesse und für die Zukunftsfähigkeit im Sinne der Plattformökonomie. Aber auch mit Blick auf die Nachhaltigkeit kommt der Cloud eine besondere Rolle zu, ermöglicht sie schließlich eine klimaschonende Digitalisierung.

Es wird jedenfalls deutlich: Ohne Cloud geht (fast) nichts mehr. Aber wie gelingt eine erfolgreiche Cloud-Transformation? In jedem Fall erfordert sie eine sorgfältige Planung, Umsetzung und einen ganzheitlichen Ansatz, der sowohl Business- als auch IT-Ziele berücksichtigt. Schließlich geht es nicht nur darum, Rechenkapazitäten in die Cloud zu verschieben, sondern auch um die Neugestaltung von Prozessen, die Modernisierung von Anwendungen und die Berücksichtigung von Sicherheitsaspekten. Auch spielen Themen wie regulatorische Anforderungen, Mindset & Change sowie das regelkonforme Management von Cloud-Umgebungen eine wichtige Rolle. Für viele Unternehmen ist dies eine große Herausforderung, denn es fehlen Cloud-Experten und -Expertinnen sowie ganz praktische Erfahrungen.

Die neue Ausgabe des Lünendonk®-Magazins beschäftigt sich mit dem umfassenden Themenkomplex der Cloud-Transformation. Dabei wird nicht nur auf die technologische Perspektive, sondern auch auf die Anforderungen und Herausforderungen bei der Nutzung von Cloud-Services näher eingegangen. Neben Lünendonk-Analysten skizzieren erfahrene Führungskräfte von Digital- und IT-Beratungen die Bedeutung der Cloud und zeigen praxiserprobte Lösungen auf.

Ich wünsche Ihnen eine interessante Lektüre!

Mario Zillmann,
Partner
Lünendonk & Hossenfelder GmbH

Inhalt

Digitalisierung & Cloud-Transformation

Cloud-Transformation – Element der digitalen Transformation
Von Mario Zillmann 6

Die Zukunft der Anwendungsmodernisierung und Cloud-Transformation
Von Friederike Frommann und Sebastian Paas 12

„Eat your own dog food"
Interview mit Christian Krause 16

Change & Mindset

FinOps – ein Vorgehensmodell für optimierte Cloud-Kosten
Von Dr. Stefan Schnitter 20

Warum es an der Zeit ist, Consulting neu zu denken
Von Thilo Mundt 24

Cloud Transformation – Practices

Edge Computing ist ein Enabler für Echtzeit, Datenschutz und Nachhaltigkeit
Interview mit Benjamin Springub und Dr. Stefan Schnitter 28

Erfolgreiche Cloud-Migration: Die Applikation steht im Mittelpunkt
Von Marcus Neumann 32

International wachsen durch Cloud-Technologie – darauf sollten Unternehmen achten
Von Dr. Manuel Audi 38

Governance ist der Schlüssel zu sicheren und nachhaltigen Cloud-Lösungen
Interview mit Marcus Neumann 42

Compliance & Security

Herausforderungen der Cloud-Transformation
Von Mario Zillmann 46

Compliance und Sicherheit der Cloud-Transformation – die geteilte Verantwortung im Blick behalten
Von Jörg Botsch und Aleksei Resetko 50

Cloud Security – individuelle Risiken und effektive Maßnahmen
Von Jens Westphal 54

STANDARDS

Editorial 3
Autorenprofile, Interviewprofile und Unternehmensprofile 58
Impressum 67

06

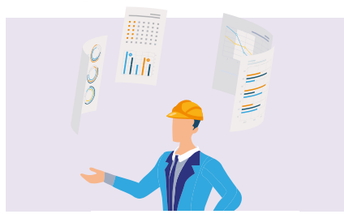
Cloud-Transformation – Element der digitalen Transformation

16

„Eat your own dog food"

20

FinOps – ein Vorgehensmodell für optimierte Cloud-Kosten



32

Erfolgreiche Cloud-Migration: Die Applikation steht im Mittelpunkt

42

Governance ist der Schlüssel zu sicheren und nachhaltigen Cloud-Lösungen

54

Cloud Security – individuelle Risiken und effektive Maßnahmen

Cloud-Transformation – Element der digitalen Transformation

Von Mario Zillmann

Keine digitale Transformation ohne Cloud-Transformation. Wie bei vielen anderen Digitalisierungsthemen hat auch die Coronakrise in sehr vielen Unternehmen und Organisationen zu einem Umdenken beim Thema Cloud geführt. Tatsächlich zeigen diverse Studien, dass es oftmals keine echte Alternative zur Nutzung von Cloud-Diensten gibt – zumindest dort nicht, wo es um die Stärkung der Innovations- und Wettbewerbsfähigkeit sowie um digitale Geschäftsmodelle geht.

Anforderungen aus dem Business an die IT

Die digitale Transformation verlief lange Zeit im deutschsprachigen Raum eher langsam und vorwiegend in einzelnen Unternehmensbereichen statt unternehmensweit. Während der Fokus sehr stark auf der Digitalisierung bestehender Prozesse im Sinne von Prozesseffizienz lag, wurden die digitale Transformation der Geschäftsprozesse und Geschäftsmodelle sowie die Innovationsentwicklung oft nicht hoch genug priorisiert. Seit dem Jahr 2020 erhöhte sich aber nicht nur der Druck zur Transformation, sondern auch die Geschwindigkeit bei ihrer Umsetzung.

Vor allem die durch die Pandemie gestörten physischen Absatz- und Kommunikationskanäle haben digitale Kanäle für Verbraucher und Verbraucherinnen erstmals notwendig und auch nach dem Abklingen der Pandemie unentbehrlich gemacht. Gleichzeitig wurde in den letzten Jahren in Regionen wie China die Revolution der Industrie 4.0 und des Internet of Things massiv vorangetrieben. Datenbasierte Geschäftsmodelle sind dort mittlerweile Realität geworden.

Für die Mehrheit der Unternehmen führen diese Entwicklungen aber dazu, dass sie sich nun den veränderten Kunden- und Marktanforderungen stellen müssen. Daher haben sich die Anforderungen an die IT stark verändert (siehe Grafik 1). Großer Druck für Veränderungen besteht vor allem hinsichtlich der Erhöhung von Kundenzentrierung und Prozesseffizienz. So erwartet das Business in acht von zehn Unternehmen von der IT neben kürzeren Reaktionszeiten und mehr Innovationsstärke auch eine deutlich höhere Performance der IT-Landschaft. Da der Geschäftserfolg immer mehr von digitalen Lösungen abhängt, ergeben sich neue Anforderungen an die IT-Operations wie Aktualität, Skalierung und Security, aber auch eine 24/7-Verfügbarkeit und ein hoher Automatisierungsgrad.

Die IT muss auf viele Business-Anforderungen gleichzeitig reagieren

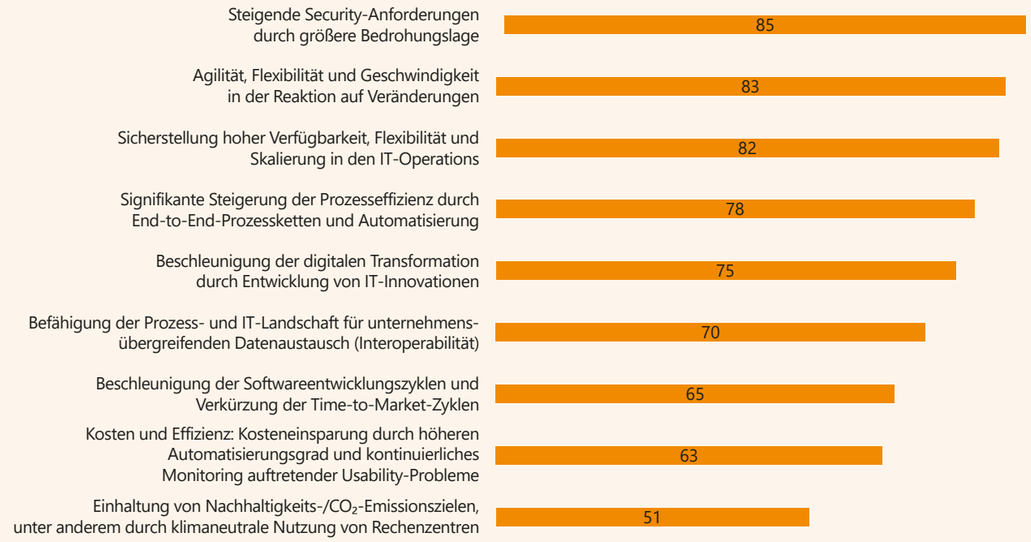
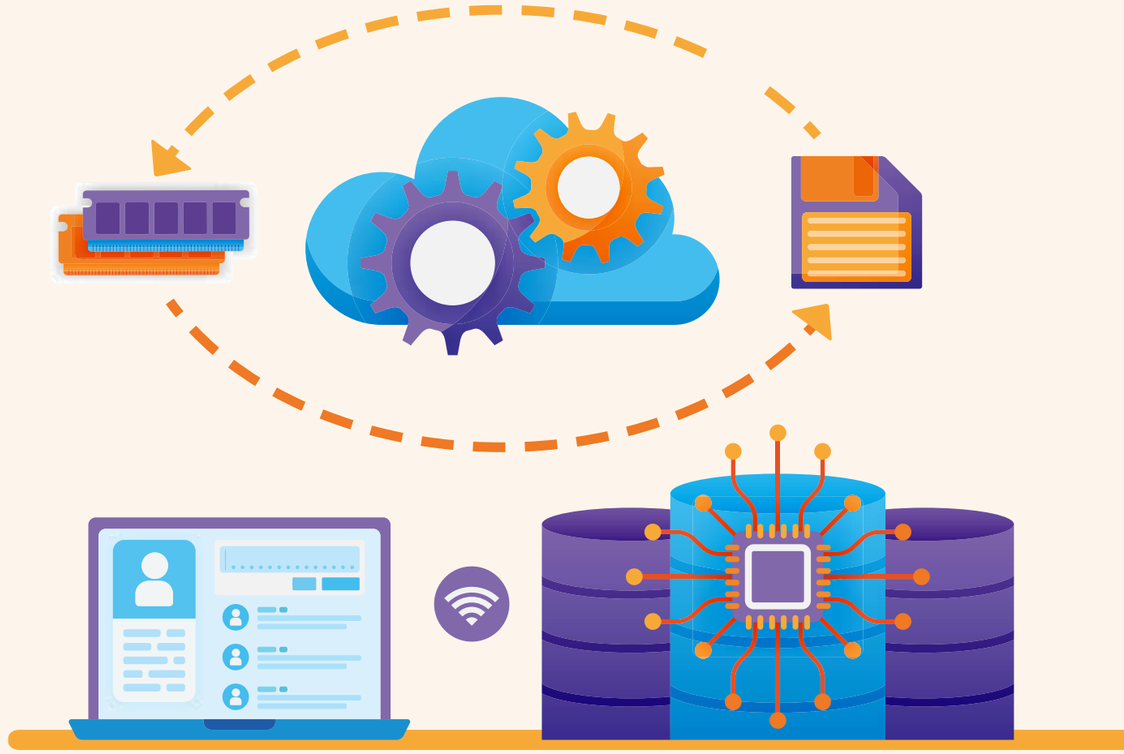


ABB. 1.1: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-DIENSTLEISTUNGEN IN DEUTSCHLAND" 2023, FRAGE: AUF WELCHE DER FOLGENDEN BUSINESS-ANFORDERUNGEN MUSS DIE IT IN IHREM UNTERNEHMEN IN DEN KOMMENDEN ZWEI JAHREN VERSTÄRKT REAGIEREN?; SKALA VON 1=„GAR NICHT" BIS 4=„SEHR STARK"; WERTE BEZIEHEN SICH AUF DIE ANTWORTEN „STARK" BIS „SEHR STARK"; N = 115



Unternehmen erhöhen ihren Cloud-Reifegrad

Ohne die Nutzung von Cloud-Services werden die meisten dieser Anforderungen allerdings gar nicht zu erfüllen sein. Tatsächlich stiegen im Zeitraum ab 2020 laut Lünendonk-Analysen die Ausgaben für IT-Modernisierungs- und Cloud-Transformationsprojekte signifikant an. Auch 2024 und 2025 richtet jedes zweite Unternehmen einen starken Fokus auf die Cloud-Transformation.

Definition „Cloud-native“

„Cloud-native“ beschreibt einen Ansatz in der Softwareentwicklung, bei dem Applikationen von Anfang an für den Einsatz in der Cloud konzipiert oder – im Fall von IT-Legacy-Anwendungen – entsprechend umgebaut werden (z. B. Re-Architecturing, Re-Platforming). Cloud-native-Anwendungen können sowohl in der Public als auch in der Private Cloud betrieben werden.

IT-Investitionsschwerpunkte 2024-2025

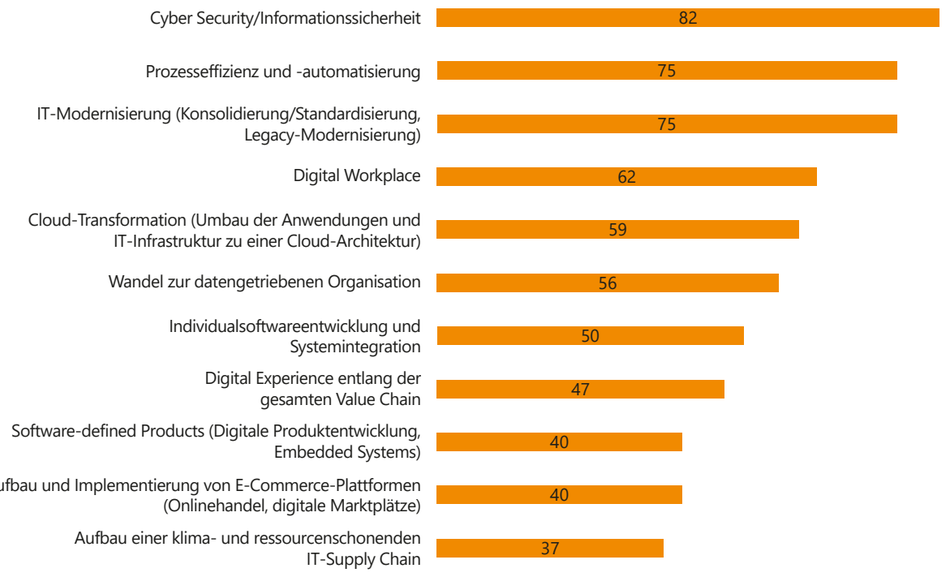


ABB. 1.2: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-DIENSTLEISTUNGEN IN DEUTSCHLAND“ 2023, FRAGE: IN WELCHE THEMEN INVESTIERT IHR UNTERNEHMEN IN DEN KOMMENDEN ZWEI JAHREN?; SKALA VON 1=„GAR NICHT“ BIS 4=„SEHR STARK“; WERTE BEZIEHEN SICH AUF DIE ANTWORTEN „STARK“ BIS „SEHR STARK“; N = 113

Im Zuge der Digitalisierungsstrategien wird die Cloud immer mehr zu einem zentralen strategischen Element. Während in den Jahren vor Corona vor allem IT-Infrastruktur aus der Cloud genutzt oder einzelne Anwendungen via „Lift & Shift“-Ansatz in die Cloud migriert wurden, findet nun ein Umbau der in die Jahre gekommenen IT-Landschaften zu Cloud-native-Architekturen statt. Der wesentliche Treiber dieser Entwicklung sind die veränderten Anforderungen, die sich im Zuge der Digitalisierung an die IT-Landschaften ergeben – vor allem hinsichtlich Dateninteroperabilität, Skalierung und Performance. Aber auch Security-Aspekte gelten immer häufiger als Argument für die Cloud-Transformation.

Cloud-Transformationsstrategien: so viel Cloud wie möglich, so wenig on Premise wie nötig

13 Prozent der Unternehmen verfolgen bei ihrer Cloud-Transformation konsequent eine Cloud-only-Strategie, sodass ausschließlich Cloud-Services bezogen werden und „on Premise“ gar keine Rolle mehr spielt. Unter den Unternehmen aus der Größenordnung von über einer Milliarde Euro Umsatz verfolgt sogar jedes fünfte Unternehmen (21 %) eine Cloud-only-Strategie.

45 Prozent der Unternehmen verfolgen dagegen eine Cloud-first-Strategie. Das heißt, sie bevorzugen zwar grundsätzlich Cloud-Lösungen, jedoch nutzen sie für bestimmte Anwendungsfälle weiterhin On-Premise-Lösungen. „Cloud first“ wird auch hier von größeren Unternehmen präferiert: 53 Prozent der Unternehmen mit einem Umsatz von über einer Milliarde Euro setzen darauf. Bei Unternehmen mit einem Umsatz von 500 Millionen bis einer Milliarde Euro liegt der Anteil bei 51 Prozent. Dagegen verfolgen nur 36 Prozent der mittelständischen Unternehmen mit einem Umsatz von bis zu 500 Millionen Euro eine Cloud-first-Strategie.

Noch mehr Entscheidungsfreiraum nehmen sich 39 Prozent der Teilnehmerunternehmen, indem sie einen Cloud-too-Ansatz verfolgen. Jedes zweite Unternehmen der Umsatzklasse von 100 bis 500 Millionen Euro verfolgt diese Strategie. Im Branchenvergleich streben Industrieunternehmen häufiger eine Cloud-too-Strategie an als Unternehmen anderer Branchen. Bei einer Cloud-too-Strategie werden Anwendungen oder Kapazitäten in die Cloud verlagert oder es wird Software as a Service (SaaS) bezogen. Grundsätzlich gibt es hier aber keine Präferenz gegenüber der Cloud, sondern es wird situativ entschieden – also ein hybrider Ansatz.

Nahezu alle Unternehmen verfolgen eine klare Cloud-Strategie

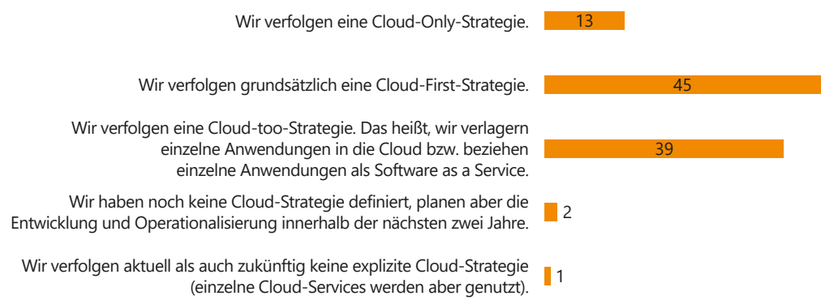


ABB. 1.3: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, FRAGE: WELCHE ART VON CLOUD-STRATEGIE VERFOLGT IHR UNTERNEHMEN?; ALLE TEILNEHMER; N = 119

Cloud-native wird Basis für Softwareentwicklung

Im Zuge der digitalen Transformation spielen Cloud-native-Technologien nicht nur bei der IT-Modernisierung, sondern auch in der Innovations- und Softwareentwicklung eine immer größere Rolle. Laut Lünendonk-Research versprechen sich tatsächlich acht von zehn Unternehmen von der Cloud eine Erhöhung ihrer Innovationskraft und nutzen Cloud-native-Technologien als Grundlage für die Entwicklung digitaler Produkte. Dabei werden Cloud-native-Technologien vor allem und in hohem Maße dort eingesetzt, wo besonders hohe Anforderungen an Skalierbarkeit und Verfügbarkeit bestehen (z. B. bei Frontend-Anwendungen im Online-Geschäft) sowie in jenen Bereichen, in denen viel experimentiert wird und IT-Ressourcen daher schnell und auch günstig verfügbar sein müssen (z. B. in der Produktentwicklung, im Vertrieb oder im Marketing). Vor diesem Hintergrund beobachtet Lünendonk eine rasant steigende Nachfrage nach Entwickler-Tools und IT-Infrastrukturkomponenten aus Public-Cloud-Plattformen wie Serverless-Architekturen, Infrastructure as Code oder Container.

Laut Lünendonk®-Studie „Cloud, Data & Software“ bauen 27 Prozent der befragten Unternehmen einen Großteil ihrer Anwendungen zu einer Cloud-native-Plattform um, während weitere 30 Prozent eine entsprechende Transformation der IT-Landschaft planen. 45 Prozent der Befragten gaben darüber hinaus an, dass sie mit dem Umbau einzelner Teile ihrer Legacy-Landschaft begonnen und sich damit auf die Cloud-Journey begeben haben. Dem gegenüber stehen jedoch 28 Prozent der Unternehmen, die einen Großteil ihrer Anwendungen zunächst nur per Lift & Shift in die Cloud überführen – also keine Anpassungen an der Architektur vornehmen. Der Trend zur Cloud-native-Softwareentwicklung wird dadurch bestätigt, dass 36 Prozent der Unternehmen bei der Entwicklung neuer Softwarelösungen bevorzugt auf Cloud-native-Technologien setzen.

Cloud-Transformation ist wichtiges Element für nachhaltige IT

Wenn immer mehr Unternehmen in ihre digitale Transformation investieren, nutzen sie deutlich mehr IT-Ressourcen. Damit nimmt jedoch der CO_2-Fußabdruck der IT stark zu. Im Zuge der gesetzlichen Regelungen rund um das Reporting von Nachhaltigkeitszielen (ESG) steigt folglich der Druck, bei zunehmender Digitalisierung auch Nachhaltigkeitsaspekte in den Business Models der Zukunft zu berücksichtigen.

Mit Blick auf den IT-Fußabdruck wird in Zukunft mehr auf einen effizienten Einsatz von Ressourcen geachtet werden müssen. Das bedeutet unter anderem, in der Softwareentwicklung nur Features zu entwickeln, die auch tatsächliche Kundenprobleme lösen oder zu Effizienzsteigerungen und Produktivitätsverbesserungen führen. Laut Lünendonk®-Studie 2023 „Der Markt für IT-Dienstleistungen in Deutschland“ spielt die Cloud für 41 Prozent der befragten IT-Verantwortlichen eine zentrale Rolle für die Reduzierung von CO_2-Emissionen. So nutzen etwa die Cloud-Anbieter immer mehr regenerative Energiequellen für die Versorgung ihrer Rechenzentren, was die Ökobilanz von Cloud-Diensten insgesamt verbessert. Darüber hinaus ermöglicht es die Cloud, unter anderem durch KI-basierte Steuerungstools im Capacity-and-Performance-Management die tatsächlich benötigten IT-Ressourcen effizienter zu nutzen und so Rechenleistung und Energie zu sparen.

Die meisten Unternehmen stehen bei der Cloud-Transformation aber noch am Anfang

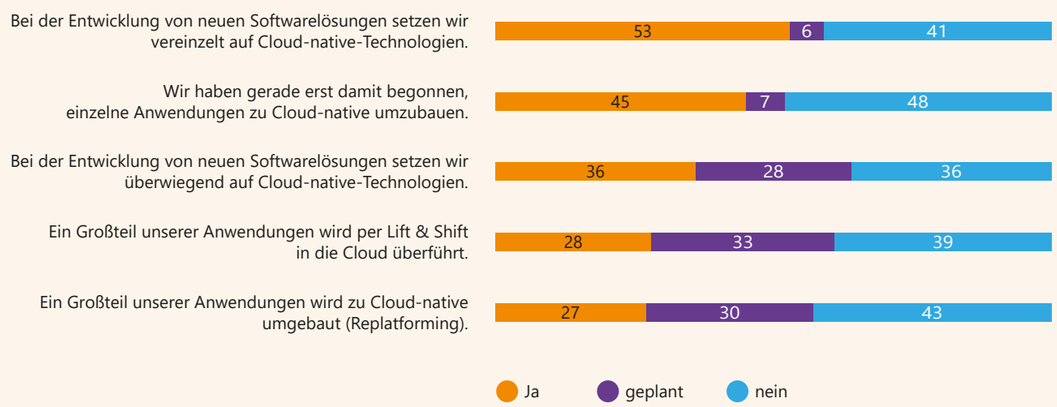


ABB. 1.4: LÜNENDONK®-STUDIE „CLOUD, DATA & SOFTWARE – DER KERN DER DIGITALEN TRANSFORMATION“ 2023, FRAGE: WO STEHT IHR UNTERNEHMEN BEI DER CLOUD-TRANSFORMATION? ALLE TEILNEHMER; HÄUFIGKEITSVERTEILUNG; N = 150

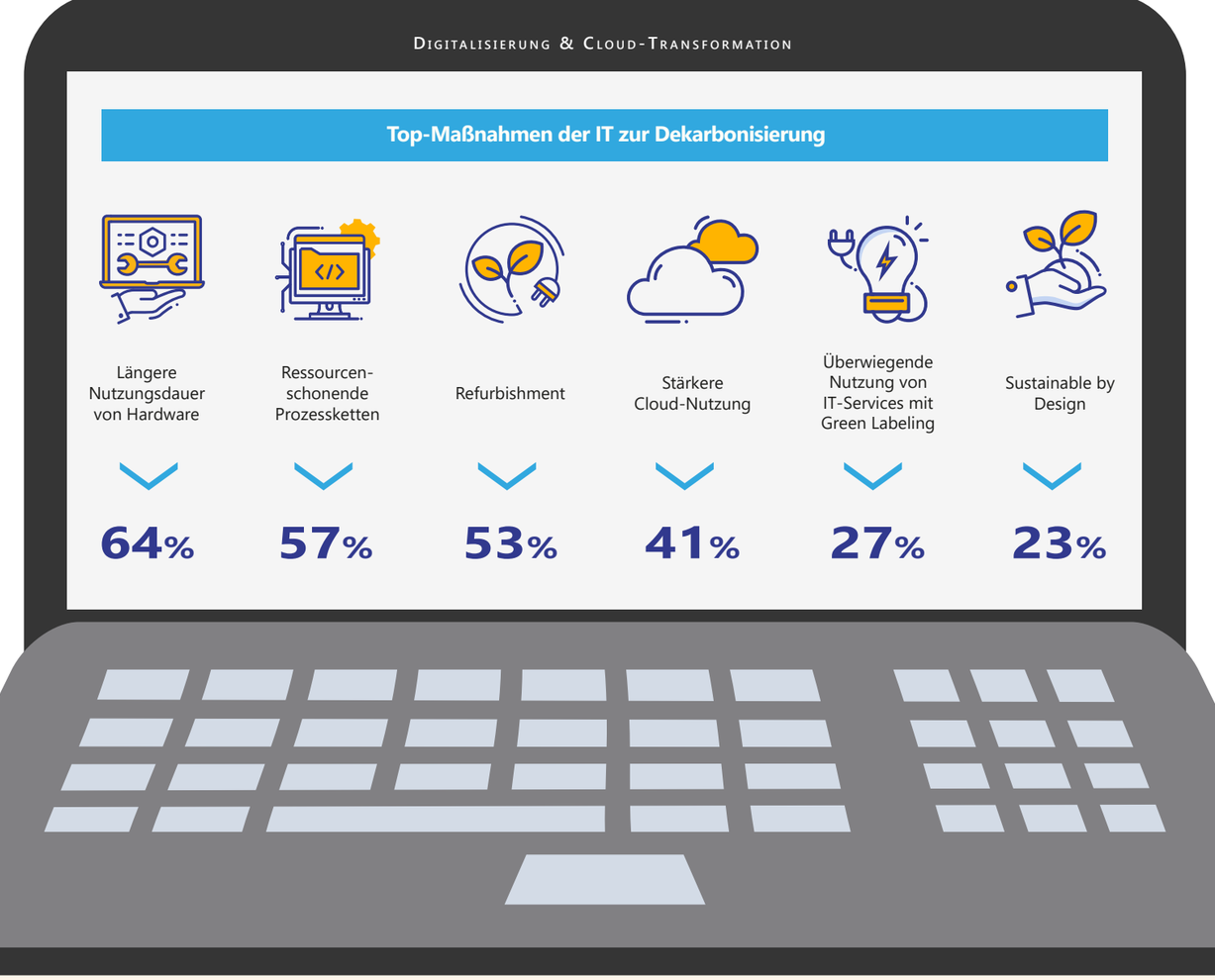


ABB. 1.5: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-DIENSTLEISTUNGEN IN DEUTSCHLAND“ 2023, FRAGE: WAS SIND DIE TOP-MASSNAHMEN IN IHREM UNTERNEHMEN FÜR DIE DEKARBONISIERUNG?; ALLE TEILNEHMER; N = 116

Fazit und Ausblick

Der Trend zu Cloud-native-Technologien wird unter anderem dadurch getrieben, dass derzeit gerade mittelständische Unternehmen unter großem Druck stehen, mit der technologischen Entwicklung Schritt zu halten, Prozesse zu digitalisieren oder Innovationen und digitale Produkte zu entwickeln. Ihnen fehlen jedoch oft die Ressourcen für die Bereitstellung skalierbarer und hoch verfügbarer Rechenleistung oder den Aufbau von Private-Cloud-Umgebungen, weshalb sie immer häufiger Cloud-native-Dienste aus der Public Cloud nutzen. Aber auch Großunternehmen und Konzerne setzen im Zuge ihrer Digitalstrategien sehr stark auf Cloud-native und in diesem Zusammenhang auf die Lösungen der Hyperscaler (AWS, Google Cloud, Microsoft Azure), wohingegen im Mittelstand oder auch in den KRITIS-Branchen (kritische Infrastruktur) noch größere Vorbehalte gegenüber den Hyperscalern bestehen. Hier wird daher die Diskussion über souveräne Clouds nach europäischem Recht immer intensiver geführt und lokale Cloud-Anbieter wie Plusserver oder StackIT treten in den Markt ein, während gleichzeitig auch die Hyperscaler mit europäischen IT-Dienstleistern in Verhandlungen über Treuhändermodelle sind.

Mit zunehmender Digitalisierung und dem Eintritt in digitale Geschäftsmodelle werden sich die Geschäftsprozesse immer stärker zu intelligent gesteuerten und automatisierten End-to-End-Prozessketten verändern. Dies erfordert eine hohe Skalierbarkeit, Flexibilität und Performance. Ohne eine – zumindest in Teilen – Cloud-native-Architektur bei vielen der unterstützenden Softwareanwendungen werden diese Ziele nicht oder nur eingeschränkt zu erreichen sein. Durch die Nutzung von Cloud-Services wollen viele Unternehmen zusätzliche Innovationen ermöglichen, was sich in der steigenden Nachfrage nach externer Unterstützung bei der Cloud-Transformation widerspiegelt.

Die Zukunft der Anwendungsmodernisierung und Cloud-Transformation: Innovationspotenzial und Vorteile für Unternehmen

Von Friederike Frommann und Sebastian Paas

Die Modernisierung von Anwendungen ist ein wichtiger Motor für zukünftige Innovationen und digitale Transformationen

In den letzten Jahren wurde die Entwicklung der IT-Infrastruktur maßgeblich durch den Umstieg in die Cloud und den verstärkten Einsatz von Cloud-Lösungen vorangetrieben. Die digitale Transformation von Geschäftsprozessen erfordert oft umfangreiche Anpassungen von Geschäftsanwendungen, die häufig nicht optimal integriert sind. Unternehmen suchen zunehmend nach Möglichkeiten, ihre Geschäftsprozesse mithilfe von Technologie zu verbessern, um Lösungen schneller und kostengünstiger zu implementieren und gleichzeitig eine optimierte Benutzererfahrung zu ermöglichen. Derzeit stehen viele Unternehmen vor der Herausforderung, veraltete Systeme zu ersetzen, die aufgrund mangelnder Integration, Benutzerfreundlichkeit, auslaufenden Supports und fehlender Anpassungsfähigkeit nicht mehr den Anforderungen entsprechen.

Public-Cloud-Lösungen bieten einzelnen Geschäftsbereichen oft signifikante Vorteile: Verkürzte Markteinführungszeiten und die schnelle Reproduktion von Produktionssystemen tragen wesentlich zur Steigerung der Innovationskraft bei. Die einfache Integration und das problemlose Testen neuer Technologien in Cloud-Systemen ermöglichen agilen DevOps-Teams den Aufbau und Test neuer Infrastrukturen und Technologien ohne zusätzliche Kosten oder Risiken. Die Nutzung von Cloud-Lösungen bietet Zugang zu einer Vielzahl von Diensten und ermöglicht gleichzeitig Flexibilität. Dies hat zu einem deutlichen Anstieg der weltweiten Ausgaben für Cloud-Technologien geführt (Statista, 2022).

Trotz der breiten Akzeptanz von Cloud-Diensten in allen Branchen wissen jedoch viele Unternehmen noch nicht, wie sie das volle Potenzial der Cloud optimal nutzen können. Zudem setzen viele Unternehmen immer noch eine Vielzahl veralteter Anwendungen ein, die auf überholten Technologien basieren. Dies schränkt die Skalierbarkeit, Flexibilität und Kompatibilität mit modernen Plattformen deutlich ein.
Unsere eigene Erfahrung zeigt, dass die einfache Übernahme und Migration von Anwendungen in eine Infrastructure-as-a-Service(IaaS)-Umgebung nicht unbedingt die beste Vorgehensweise ist. Stattdessen empfiehlt es sich, eine Cloud-native Architektur zu entwickeln, um alle Vorteile der Public Cloud optimal zu nutzen und damit den aktuellen Anforderungen gerecht zu werden.

Innovative App-Modernisierung und Cloud-Optimierung: PwC und Microsoft Power Platform bieten maßgeschneiderte Lösungen für Unternehmen

Die App-Modernisierung ist für Unternehmen entscheidend, da sie veraltete Anwendungen durch moderne Lösungen ersetzt. Die Wirtschaftsprüfungs- und Beratungsgesellschaft PwC Deutschland (PwC) bietet das Tool Decommissioning as a Service an, das dank KI-Technologie veraltete und nicht verwendete Server identifizieren kann. Die Modernisierung verbessert die Agilität und Benutzererfahrung, spart Kosten, ermöglicht die Integration neuer Technologien und gewährleistet Sicherheit und Compliance. Die Umstellung von monolithischen Anwendungen auf eine mikroservicebasierte Architektur ist ein Beispiel für die App-Modernisierung. Dabei können unterschiedliche Technologien und Programmiersprachen für verschiedene Services verwendet werden, was die Flexibilität und Skalierbarkeit erhöht. Durch die Aufteilung der Anwendung in unabhängige Mikroservices können diese individuell entwickelt, bereitgestellt und skaliert werden, was zu einer effizienteren Wartung und Skalierung führt.

Für die App-Modernisierung und Cloud-Migration setzt PwC auf eine bewährte Methodik, Best Practices, Industriestandards sowie etablierte Tools, um eine maßgeschneiderte Ende-zu-Ende-Modernisierungsstrategie zu entwickeln. Dazu gehören unter anderem die Microsoft Power Platform und der sogenannte 7R-Migrationsprozess. Sie unterstützen Unternehmen dabei, vorhandene Anwendungen erfolgreich zu modernisieren und ihre gesamte Cloud-Umgebung zu optimieren. Sie zeigen zudem auf, welche Innovationen Unternehmen freilegen können, sobald sie die Cloud eingeführt haben. Ziel ist es, bestehende Anwendungen zu transformieren und zu aktualisieren, um aktuellen Marktanforderungen gerecht zu werden. Dadurch verbessert sich die Benutzerfreundlichkeit, Sicherheit und Compliance, während technische Schulden reduziert werden.

Die Microsoft Power Platform ist eine Sammlung von Tools und Diensten, die es Unternehmen ermöglicht, leistungsstarke Lösungen für Automatisierung, Datenanalyse und Anwendungsentwicklung zu erstellen. Sie umfasst vier Hauptkomponenten: Power Apps, Power Automate, Power BI und Power Virtual Agents. Power Apps ermöglicht die Erstellung benutzerdefinierter Apps ohne umfangreiche Codierung. Power Automate automatisiert Geschäftsprozesse und Workflows, während Power BI Datenvisualisierung und Business Intelligence bietet. Power Virtual Agents ermöglicht die Entwicklung intelligenter Chatbots. Durch die Nutzung der Power Platform können Unternehmen ihre Effizienz steigern, Kosten senken und schnell auf sich ändernde Geschäftsanforderungen reagieren.

Der 7R-Cloud-Migrationsprozess ist ein bewährter und angepasster Ansatz für eine erfolgreiche App-Modernisierung und -migration. Er umfasst sieben Prozessschritte: Retire, Rehost, Retain, Replace, Refactor, Replatform und Reimagine. Jeder Schritt hat eine spezifische Funktion und trägt zum reibungslosen Übergang der Anwendungen in die Cloud bei. Durch eine sorgfältige Umsetzung dieses Prozesses können Unternehmen sicherstellen, dass ihre Applikationen nahtlos in eine neue Umgebung überführt werden, was potenzielle Probleme und Ausfallzeiten minimiert.

Cloud-Innovationen und Generative AI: beschleunigte App-Modernisierung, IoT-Potenziale und datengesteuerte Innovationen

Die Cloud bietet Unternehmen zahlreiche Innovationsmöglichkeiten, insbesondere in Bezug auf Skalierbarkeit, Verfügbarkeit, Ausfallsicherheit, Sicherheit und Compliance. Durch die Nutzung der Public Cloud können Unternehmen ihre Anwendungen bei hohem Datenverkehr skalieren und eine kontinuierliche Verfügbarkeit gewährleisten. Zudem bietet die Cloud Sicherheitsfunktionen und -tools, um Bedrohungen entgegenzuwirken und Compliance-Anforderungen zu erfüllen. Ein umfassendes Überwachungssystem ermöglicht es, potenzielle Engpässe oder Leistungsprobleme frühzeitig zu erkennen. Trotz der Compliance-Standards der Cloud-Provider sind Cloud-Nutzer letztendlich allerdings selbst für die Einhaltung von Compliance-Vorschriften und Sicherheitsmaßnahmen verantwortlich.

Unsere Expertinnen und Experten beobachten immer mehr eine Dezentralisierung und Standardisierung der IT-Infrastruktur durch den Einsatz von Cloud-Lösungen. Durch die Verlagerung von IT-Ressourcen in die Cloud entlasten Unternehmen ihre interne Infrastruktur und können sich verstärkt auf strategische Aufgaben und Innovation konzentrieren. Die Nutzung von Generative AI wie ChatGPT und Copilot bietet Unternehmen vielfältige Möglichkeiten zur Entwicklung neuer Produkte, Dienstleistungen und Geschäftsmodelle. Generative AI beschleunigt die Modernisierung von Apps und ermöglicht die schnelle Generierung neuer Ideen und Lösungen. Die Automatisierung von wiederholbaren Aufgaben und Prozessen durch Generative AI in Verbindung mit KI-Techniken wie maschinellem Lernen und Robotik optimiert Arbeitsabläufe, steigert die Effizienz und reduziert die Arbeitsbelastung. KI-basierte Analysen liefern wertvolle Erkenntnisse und unterstützen Unternehmen bei der Bereitstellung maßgeschneiderter Produktangebote zur Verbesserung des Kundenerlebnisses und der Kundenbindung. Generative AI bietet als leistungsstarkes Werkzeug Unternehmen das Potenzial, Modernisierungsprozesse zu beschleunigen und schneller innovative Lösungen zu entwickeln und damit beispielsweise neue Märkte zu erschließen.

Das Internet of Things (IoT) vernetzt Geräte mithilfe von Sensorik und Software, um Daten zu sammeln, zu analysieren und eine Kommunikation zwischen den Geräten herzustellen. Die Cloud spielt eine entscheidende Rolle bei der Skalierung und Verarbeitung großer Datenmengen im IoT und ermöglicht innovative Anwendungen. Durch diese Vernetzung können Geräte Informationen erfassen, teilen und autonome Aktionen ausführen. Die Public Cloud bietet eine Plattform zur Verbindung, Verwaltung und Überwachung der Geräte und bringt Vorteile wie den Zugriff auf Daten von überall und jederzeit, Skalierbarkeit der Infrastruktur, Echtzeitanalysen und die Integration mit anderen Technologien wie künstlicher Intelligenz und maschinellem Lernen. Die Sicherheit von Daten und Geräten ist ein wesentlicher Aspekt im IoT, und die Cloud bietet fortschrittliche Sicherheitsmechanismen wie Verschlüsselung, Authentifizierung und sichere Kommunikationsprotokolle, um die Integrität und Vertraulichkeit der IoT-Daten zu gewährleisten.

Cloud-native digitale Transformation: Von der Strategie bis zur Umsetzung – Unterstützung und Beratung durch PwC

In einer zunehmend dynamischen Marktsituation und angesichts der wachsenden Nachfrage nach Cloud-Diensten wird die Bedeutung von Anwendungen in einer Cloud-native Umgebung immer deutlicher. Unternehmen, die ohne eine geeignete Modernisierungsstrategie in die Cloud wechseln, sind stark eingeschränkt in ihrer Fähigkeit, innovativ zu sein und neue Technologien in ihre Anwendungen zu integrieren.

Eine Cloud-native digitale Transformation eröffnet Unternehmen die Möglichkeit, Innovationen freizusetzen und das volle Potenzial von Cloud-Systemen auszuschöpfen. Dabei ist es jedoch entscheidend, dass die Initiative für diese Transformation aus dem Business selbst kommt und nicht allein durch technische Aspekte motiviert ist. Alle Geschäftsbereiche sollten sowohl die Chancen als auch die Verantwortung der neuen Cloud-Service-Welt kennen und verstehen.

PwC, als Bindeglied zwischen Business und IT, verfügt bereits über umfangreiche Erfahrungen in zahlreichen Transformationsprojekten. Als vertrauenswürdiger Berater steht PwC Ihnen bei Ihrer Transformation zur Seite – von der strategischen Planung bis zur erfolgreichen Umsetzung.

„Eat your own dog food“

Interview mit Christian Krause

Lünendonk: Christian Krause, Sie sind Experte für Cloud-Migrationen und helfen Ihren Unternehmenskunden dabei, moderne Service-Architekturen erfolgreich einzusetzen. Bevor wir über Ihre Aufgaben im Detail sprechen: Wie kamen Sie überhaupt zu Ihrer Passion im Cloud-Umfeld?

Christian Krause: Alles begann damit, dass ich selbst unter den Einschränkungen im Bereich IT-Infrastruktur gelitten habe. In den 90er-Jahren hatten wir es bei ERP- und Service-Systemen noch mit Hardware zu tun, die schwer, teuer und unflexibel war. Es gab Probleme bei der Erweiterung und Kunden hatten Schwierigkeiten, die richtige Kapazität zu planen. In den 2000er-Jahren begannen wir mit Application Service Providing, was schon ein großer Fortschritt war. Aber erst mit den modernen Service-Plattformen kam der Durchbruch: virtuelle Maschinen mit individueller Prozessor- und Speicherkonfiguration, beliebig skalierbar und hochflexibel. Das ist das, was mich an der Cloud fasziniert und begeistert.

Lünendonk: Skalierbarkeit und Flexibilität sind ja zwei der herausragenden Punkte, bei denen die Cloud besser abschneidet als eine interne Lösung. Allgemein gesprochen: Welche Vorteile bietet die Cloud im Vergleich zu herkömmlichen In-House-Lösungen? Und warum ist es wichtig, sich jetzt mit dem Thema auseinanderzusetzen?

Christian Krause: Tatsächlich ist die einfache Skalierbarkeit ein Gamechanger, da man sich absolut keine Gedanken mehr über Infrastrukturen machen muss. Aber die Cloud besteht nicht nur aus virtuellen Maschinen und Datenbanken, sondern sie bietet viele weitere Dienste. Unternehmen haben Zugang zu einem großen Innovationspool, der mit einer internen Lösung nicht realisierbar ist. Maschinelles Lernen, künstliche Intelligenz, Quanten-Computing – das sind alles Technologien, die Unternehmen für ihre Geschäftsentwicklung nutzen können. Zudem betreiben große Anbieter ihre Cloud-Systeme auf einem Niveau von Effizienz und Ressourcenschonung, das Unternehmen in Eigenregie nicht erreichen. Die Cloud bietet entscheidende Wettbewerbsvorteile – und Unternehmen, deren Kernkompetenz nicht die IT ist, sollten diese Vorteile nicht liegen lassen.

Lünendonk: Die technologischen Möglichkeiten klingen natürlich beeindruckend. Aber Technologie ist nur einer von vielen Faktoren, die bei Cloud-Migrationen eine Rolle spielen. Was gehört Ihrer Meinung nach zu einer guten und zielführenden Strategie, abseits von den technischen Fragen?

Christian Krause: Aus meiner Sicht besteht die Herausforderung darin, zwei Ansätze miteinander zu verbinden: den Top-down-Ansatz, der von der Organisationsstruktur und den Geschäftsprozessen ausgeht, und den Bottom-up-Ansatz, der die richtige Skalierung und Technologie berücksichtigt. Wir arbeiten mit einem speziellen Cloud-Adoption-Framework, das diese beiden Dimensionen verbindet und unseren Kunden eine klare Roadmap für ihre Cloud-Strategie und -Transformation zur Verfügung stellt. Das hat sich wirklich bewährt.

Man bekommt einen umfassenden Überblick über das Gesamtprojekt und hat zugleich Meilensteine für erfolgreich umgesetzte Teilabschnitte. Wichtig ist dabei wie gesagt, dass beide Dimensionen berücksichtigt werden: die Integration der Cloud in die Geschäftsstrategie und betriebswirtschaftliche Erfolgskriterien einerseits und andererseits die technischen Aspekte wie das Code-Management, Kosteneffizienz, Messung und Optimierung, Governance und Sicherheit.

Lünendonk: Frameworks sind das eine, etwas ganz anderes ist es aber, sie im praktischen Einsatz zu erleben. Als Berater kennen Sie die Praxis und haben viele Unternehmen bei ihrer Cloud-Migration begleitet. Wenn Sie Ihre Erfahrungen Revue passieren lassen: Welche Fehler begehen Unternehmen häufig, bewusst oder unbewusst?

Christian Krause: Ein Problem, das eher selten beschrieben wird, mir aber schon oft begegnet ist, hat mit der Abgrenzung von Produktivsystemen und Testumgebungen zu tun. Man kann tatsächlich in große Schwierigkeiten geraten, wenn unklar ist, wie weit die IT-Abteilung mit einer Testumgebung gehen darf. Man macht aus einem Testsystem vorschnell eine Mission-Critical-Infrastruktur – und plötzlich gibt es Probleme mit der Website oder dem Zugriff auf wichtige Anwendungen.

Das lässt sich allerdings recht einfach vermeiden, wenn man ein Framework einsetzt, das klare Grenzen definiert. Ein weiterer häufiger Fehler ist die Vernachlässigung von Aspekten wie Sicherheit, optimale Namenskonventionen oder Wiederholbarkeit von Cloud-Deployment-Szenarien. Auch hier kann man mit einem geeigneten Framework gegensteuern. Der Schlüssel für einen erfolgreichen Cloud-Einsatz ist die Planung im Vorfeld. Und – das sage ich jetzt ganz ohne Hintergedanken – man sollte sich erfahrene Partner ins Boot holen, die wissen, wie man solche Fehler vermeidet.

Lünendonk: Nutzen Sie eigentlich die Cloud-Lösungen, die Sie bei Ihren Kunden implementieren, auch selbst?

Christian Krause: Aber sicher. Ein Gutteil unserer Erfahrungen, die wir mit Cloud-Lösungen und -Migrationen gesammelt haben, stammt aus unserer eigenen Transformation. Wir leben nach dem Prinzip „eat your own dog food“ und empfehlen unseren Kunden nur Methoden und Technologien, die wir auch selbst nutzen. Ich glaube, anders geht es auch nicht. Man vermittelt seinen Kunden ja nicht nur das Berater-Know-how, sondern auch den Enthusiasmus und die Überzeugung, die man braucht, um ein solches Vorhaben zum Erfolg zu führen. Und das kann man nur, wenn man es gewissermaßen am eigenen Leib erfahren hat. In dem Sinne „glauben“ wir nicht nur an die Cloud, sondern wir „leben“ sie im eigenen Unternehmen – und das sehr erfolgreich.

Lünendonk: Die Cloud ist für viele Unternehmen vor allem eine Frage des Vertrauens – schließlich werden die eigenen Daten auf fremden Servern verarbeitet. Wie vertrauenswürdig ist die Cloud Ihrer Meinung nach?

Christian Krause: Das ist in der Tat ein Punkt, der in der Vergangenheit für einige Skepsis gesorgt und viele Unternehmen verunsichert hat. Aber da kann ich guten Gewissens Entwarnung geben. Tatsächlich muss man konstatieren, dass bei den großen, renommierten Anbietern die Daten in der Cloud sicherer sind als im eigenen Unternehmen. Rechtlich und vertraglich gilt sowieso: Die Daten gehören den Kunden. Daran ändert sich auch nichts durch die Cloud. Besonders sensible Daten oder Firmengeheimnisse sind verschlüsselt, und darauf hat auch der Cloud-Anbieter keinen Zugriff. Gefahr für die Datensicherheit geht vor allem vom eigenen Umgang damit und von Cyberangriffen aus. Und an diesen Stellen ist die Cloud einfach besser als alles, was man in Eigenregie machen kann.

Microsoft hat zum Beispiel ein eigenes Cybersecurity-Operations-Center mit Tausenden Mitarbeitenden weltweit, die nur damit beschäftigt sind, die Infrastrukturen vor Angriffen von außen zu schützen. Und mit modernen Cloud-Deployment-Werkzeugen und -Lösungen etabliert man automatisch eine Governance im eigenen Unternehmen, die Datenlecks verhindert und die Anwender vor Fehlern schützt.

Lünendonk: Trotzdem fühlen sich manche Unternehmen nicht wohl bei dem Gedanken, ihre Daten und IT-Infrastruktur aus der Hand zu geben. Immerhin macht man sich auf diese Weise abhängig von einem externen Anbieter. Können Sie diese Bedenken nachvollziehen?

Christian Krause: Das kann ich durchaus. Allerdings ist das eine Situation, mit der Unternehmen auch in anderen Bereichen, etwa im Lieferkettenumfeld, konfrontiert sind. Und es gibt bewährte Strategien, Risiken zu minimieren. Ein klassischer Ansatz wäre beispielsweise eine Multi-Cloud-Strategie, bei der man Dienste von unterschiedlichen Anbietern bezieht. Grundsätzlich ist aber die Abhängigkeit von Geschäftspartnern keine Schicksalsfrage. Man macht sich auch von seinem Stromanbieter abhängig, ohne ihm vollkommen ausgeliefert zu sein.

Lünendonk: Werfen Sie noch einen Blick in die Glaskugel: Welche Rolle spielt die Cloud in Zukunft? Wird es in zehn Jahren noch Unternehmen geben, die ohne Cloud auskommen?

Christian Krause: Vielleicht wird es noch Unternehmen geben, die nicht in der Cloud sind – aber sie werden die Ausnahme sein. Die Cloud ist ein wichtiger Bestandteil zukunftsfähiger Unternehmensstrategien. In zehn Jahren wird es ganz normal sein, Cloud-Services zu nutzen, um Prozesse zu optimieren, schneller, effizienter und internationaler zu agieren. Und das gilt für alle Unternehmen, vom Start-up über den Hidden Champion im Mittelstand bis zum Weltkonzern. Die Vorteile sind einfach zu groß, um sie zu ignorieren. Und wenn der Wettbewerb durch die Nutzung von Cloud-Technologien davonzieht, werden auch die letzten Skeptiker umdenken müssen. Der digitale Wandel, der stark auf Cloud-Szenarien basiert, ist ja ein globales Phänomen, dem man sich nicht entziehen kann. Die Frage ist also nicht, ob die Cloud eine wichtige Zukunftsinvestition ist – das ist sie definitiv. Es geht vielmehr darum, die für das eigene Unternehmen beste Cloud-Deployment-Strategie zu finden. Und dabei werden die nächsten zehn Jahre auch die Phase sein, in der die Weichen für die Zukunft gestellt werden.

Lünendonk: Vielen Dank für das Gespräch!

Digitalisierung & Cloud-Transformation

FinOps – ein Vorgehensmodell für optimierte Cloud-Kosten

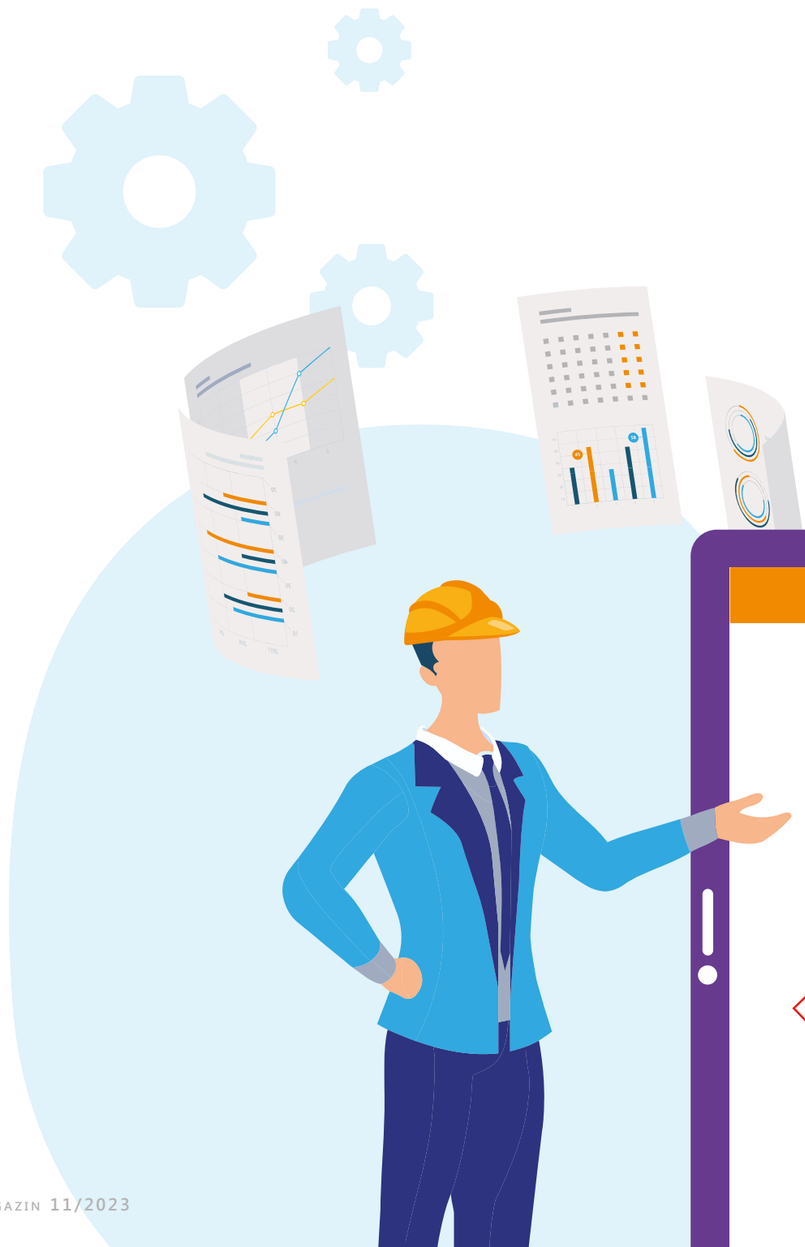
Von Dr. Stefan Schnitter

Um Cloud-Kosten im Griff zu behalten, bedarf es gesteigerter Transparenz und einer kontinuierlichen Optimierung von Cloud-Ressourcen und Kostenmanagement. Mit entsprechenden Tools und Team-übergreifendem Vorgehen ist dies möglich.

Der Weg in die Cloud ist in vollem Gange. Unternehmen versprechen sich Wachstum, Effizienz und neue Geschäftsmodelle. Allerdings geht dabei vielfach auch der Überblick über Cloud-Kosten verloren. Enthusiastisch hatten in vielen Unternehmen Teams damit begonnen, die Cloud-Transformation voranzutreiben. Jedoch stellten viele alsbald eine enorme Kostensteigerung fest. Einen unmittelbaren Ausweg gab es nicht, weil geschäftskritische Anwendungen nicht mehr einfach verlagert werden konnten. Financial Operations, kurz FinOps, geht auf diesen Mangel ein und ist ein Vorgehensmodell, das Unternehmen hilft, Cloud-Ausgaben zu optimieren. Hierfür baut es eine Brücke zwischen Finanzprozessen und Cloud Operations und berücksichtigt vor allem folgende drei Aspekte: Sichtbarkeit, Verantwortung und Optimierung.

Im ersten Schritt geht es darum, mithilfe von Tools und Prozessen mehr Transparenz in die Cloud-Nutzung und die damit verbundenen Kosten zu bringen. Die Analyse der Berichte der Tools bietet einen deutlich tieferen Einblick, wo und wie Cloud-Ressourcen genutzt werden.

Darüber hinaus ist FinOps aber auch ein Vorgehensmodell, das die unternehmensweite Verantwortung für Cloud-Kosten fördert, indem es alle Teams beteiligt. Dazu gehören etwa Business-, Einkaufs-, Finanz- und Technologieteams, die somit wie auch weitere relevante Stakeholder mehr Kontrolle über ihre Cloud-Ausgaben erlangen. Durch dynamische, regelmäßige Überwachung und datenbasierte Analysen kann FinOps zudem die Zuweisung von Cloud-Ressourcen regelmäßig anpassen und optimieren.



Warum ist Kostenmanagement in der Cloud schwierig?

Generell treten beim Kostenmanagement vor allem folgende Herausforderungen auf:

1. Transparenz von Ausgaben

Cloud-Umgebungen können sich über mehrere Anbieter, Regionen und Dienste erstrecken, was es schwierig macht, vollständige Transparenz zu erlangen. Ein umfassender Überblick über Dimensionen wie Cloud-Dienst-Nutzung, Anwendungen, Abteilungen und Projekte ist in einer Hybrid- und Multi-Cloud-Umgebung schwierig. Tools und Metriken sind häufig auf einzelne Cloud-Plattformen beschränkt und es ist schwierig, eine „End-to-End"-Transparenz bezüglich der Kosten zu schaffen.

2. Kostenoptimierung

Die Optimierung der Cloud-Kosten erfordert fundierte Kenntnisse über Dienste, Preismodelle und Konfigurationen wie auch über erforderliche Überwachungs- und Governance-Mechanismen, um Einsparpotenzial umzusetzen. Große Anbieter wie beispielsweise AWS haben hier mehr als 30 Tools/Module, die für bestimmte Aspekte der Kostenoptimierung genutzt werden können.

3. Kostenzuordnung

Die Kostenzuordnung kann aufgrund mangelnder Transparenz und einer ineffizienten Zuordnungsstrategie unorganisiert und fehlerbehaftet sein. Da die Verbindung zwischen der Nutzung von Cloud-Diensten und den Besitzern dieser Dienste auf Anwendungs-, Abteilungs- und Projektebene vielfach fehlt, können Unternehmen große Teile von Cloud-Ausgaben nicht ihren Verursachern und damit nicht den entsprechenden Produkten zuordnen.

4. Kostenprognose und Budgetierung

Cloud-Kosten variieren aufgrund von Nachfrageschwankungen, sich ändernden Servicepreisen und Nutzungsmustern, was Kostenprognosen schwierig macht. Verschiedene Preismodelle wie On-Demand-, reservierte und Spot-Instanzen erhöhen die Komplexität solcher Prognosen.

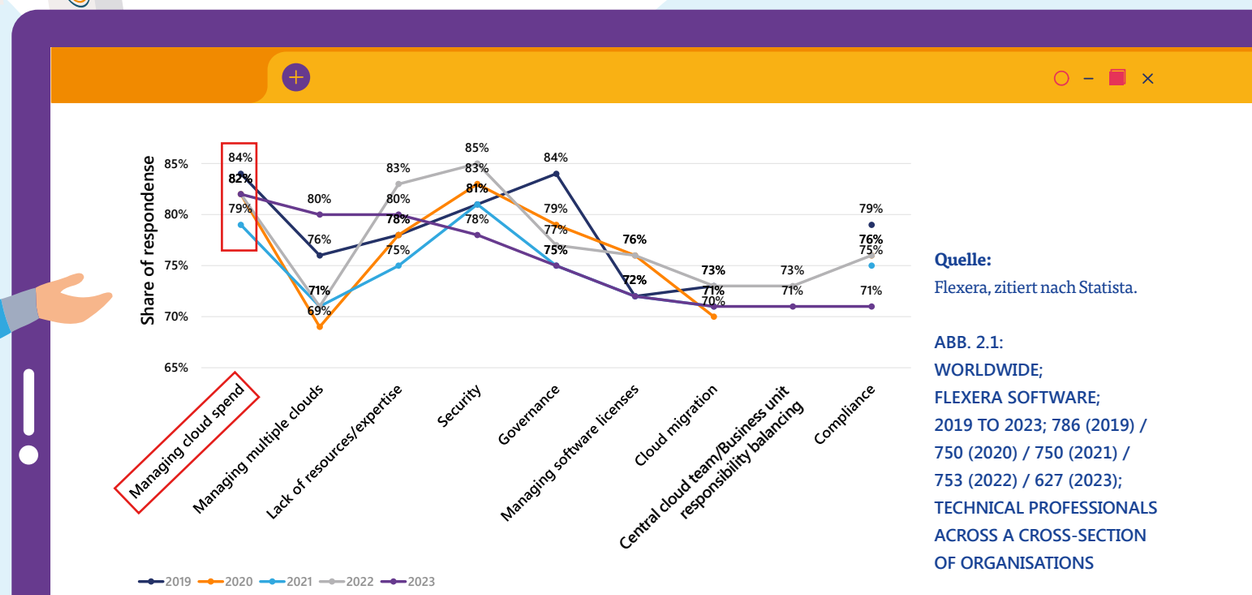
5. Governance und Compliance

Das Fehlen geeigneter Governance-Richtlinien und zugehöriger Kontrollen kann zu Verschwendungen in der Cloud führen und Unternehmen sogar vor rechtliche Probleme stellen. Bisherige Governance-Frameworks sind zudem kaum für dynamische Ausgabenmodelle geeignet. Sie konzentrieren sich vielmehr auf Leitplanken und Genehmigungsprozesse, was aber den Mehrwert der Cloud-Nutzung einschränkt.

6. Kultur der Kostenoptimierung

Das häufige Fehlen einer Kultur zur Übernahme von Kostenverantwortung führt zu Mehrausgaben in der Cloud.

Die Relevanz von FinOps wurde dabei schon in vielen Studien nachgewiesen. Basierend auf einer kürzlich erschienenen weltweiten Umfrage aus dem Jahr 2023 ist Kostenmanagement eine der größten Schwierigkeiten beim Cloud Computing



Quelle:
Flexera, zitiert nach Statista.

ABB. 2.1:
WORLDWIDE;
FLEXERA SOFTWARE;
2019 TO 2023; 786 (2019) / 750 (2020) / 750 (2021) / 753 (2022) / 627 (2023);
TECHNICAL PROFESSIONALS ACROSS A CROSS-SECTION OF ORGANISATIONS

FinOps kann zudem sicherstellen, dass Entscheidungen über Cloud-Ausgaben mit den Geschäftszielen des Unternehmens übereinstimmen. Im Gegensatz zu den traditionellen IT-Kostenmanagement-Praktiken, bei denen die Kosten nicht dynamisch gesteuert und auf einer breiteren Unternehmensebene visualisiert werden, fördert FinOps die Darstellung der Kosten (Showback) und der Kostenstellenrechnung (Chargeback) in Echtzeit. Diese Transparenz bezieht insbesondere auch die Cloud-Nutzer selbst mit ein, die beispielsweise über Kollaborationsplattformen wie Slack Echtzeitinformationen über Kostenauswirkungen und individuelle Optimierungsempfehlungen erhalten können.

Skalierbarkeit und Flexibilität sind die Haupteigenschaften von Cloud-Diensten, aber sie können zu unerwarteten Kosten in Form von Budgetüberschreitungen führen, wenn sie nicht richtig orchestriert werden. FinOps visualisiert daher Cloud-Ausgaben und Ressourcennutzung und beseitigt die Silos zwischen den verschiedenen Finanz-, Business-, Technologie- und Einkaufsteams. Dies bringt auch erhebliche Veränderungen mit sich (Abbildung 2.2). Dazu gehören erhöhte Kostentransparenz, funktionsübergreifende Zusammenarbeit, individuelle Verantwortung, kontinuierliche Optimierung sowie ein allgemeiner kultureller Wandel hin zu effektivem Kostenmanagement.

Kultureller Wandel
Mentalitäts- und Verhaltensänderung im Unternehmen durch Förderung einer Kultur der Transparenz, Zusammenarbeit, Verantwortlichkeit und kontinuierlichen Verbesserung.

Datengetriebene Entscheidungen
Datengestützte Entscheidungsfindung durch genaue und zeitnahe Kostendaten, Analyse von Ausgabenmustern, Identifizierung von Kostentreibern und optimierte Ressourcennutzung.

Daten-Demokratisierung
Ermöglicht Zugang zu Finanz- und Kostendaten für alle relevanten Stakeholder und fördert so fundierte Entscheidungen, effektive Zusammenarbeit und kollektive Verantwortung für die Kostenoptimierung.

Governance Framework
Einführung neuer Governance-Mechanismen, Richtlinien und Verfahren, Tagging-Strategie, Genehmigungsverfahren und Einhaltung von Best Practices und Vorschriften.

Verantwortung
Erzeugt Verantwortung und Befähigung durch gemeinsame Kostenüberwachung und -optimierung im gesamten Unternehmen.

ABB. 2.2: VERÄNDERUNGEN DURCH FINOPS

Wie führe ich FinOps in meinem Unternehmen ein?

Das FinOps Framework basiert auf einem kontinuierlichen Zyklus, dessen Implementierung mehrere Schritte umfasst, von der Schaffung von Bewusstsein bis hin zur eigentlichen Optimierung der Kosten. Ein schrittweises Vorgehen für die Einführung von FinOps könnte wie folgt aussehen:

1 **Vision und Strategie**
Erstellen Sie eine Vision für die Implementierung von FinOps und definieren Sie OKRs (Objectives and Key Results, also Ziele und Schlüsselergebnisse). Dazu gehören etwa konkrete Ziele für Kostenoptimierung und Ressourcennutzung, die Förderung der Datendemokratisierung, eine Erhöhung der Transparenz und die Sicherstellung des finanziellen Verantwortungsgefühls. Definieren Sie Key Performance Indicators (KPIs) zur Verfolgung des Fortschritts, um sicherzustellen, dass diese mit der Gesamtstrategie in Einklang stehen.

2 **Bewusstsein und Schulungen**
Der zweite Schritt besteht darin, wichtige Stakeholder, einschließlich Finanz-, Technologie-, Einkaufs- und Businessteams, über die Vorteile von FinOps aufzuklären. Hieran sollten sich zudem Schulungen zu FinOps anschließen.

3 **FinOps-Teams**
Bilden Sie ein funktionsübergreifendes virtuelles Team aus den Bereichen Finanzen, Technologie, Einkauf und Business, das für die Umsetzung der FinOps-Strategie verantwortlich ist.

4 **FinOps-Governance-Modell**
Bewerten Sie Ihr aktuelles Cloud-Kostenmanagement-Framework und identifizieren Sie Lücken und Verbesserungsmöglichkeiten. Identifizieren Sie fehlende erforderliche Fähigkeiten und definieren Sie ein neues FinOps-Governance-Modell mit dem Schwerpunkt dezentrale Verantwortung, Transparenz und datengetriebene Entscheidungsfindung.

5 **Mitarbeiterweiterbildung**
Definieren Sie Lernpfade und Schulungsprogramme, um Mitarbeitende für FinOps-Praktiken und die Verwendung von Tools zu schulen und gegebenenfalls nach den Standards der FinOps Foundation (finops.org) zu zertifizieren.

6 **Tools und Metriken**
Evaluieren und implementieren Sie relevante Tools und Metriken für das Cloud-Kostenmanagement. Hierbei sind sowohl Tools für einzelne Cloud-Umgebungen als auch Ende-zu-Ende-Tools zu berücksichtigen.

7 **Kostenzuordnungs- und Tagging-Strategie**
Erstellen Sie eine Kostenzuordnungsstrategie und implementieren Sie Mechanismen für das Tagging von Ressourcen, um Kosten bestimmten Projekten, Teams oder Abteilungen zuordnen zu können.

8 **Kostenoptimierungsmaßnahmen**
Identifizieren Sie Potenziale für Kostensenkungen, z. B. Rightsizing von Ressourcen, die Nutzung von Angeboten wie reservierten Instanzen oder Spot-Instanzen, die Implementierung von Automatisierungs- und Skalierungsstrategien sowie die Optimierung der Speicher- und Datenübertragungskosten.

9 **Optimierungsschleife**
Verwenden Sie iterative Ansätze, um Cloud-Kosten und Leistungsmetriken kontinuierlich zu überwachen und so Verbesserungspotenziale zu identifizieren. Bewerten Sie regelmäßig die Wirksamkeit von FinOps-Initiativen, passen Sie Strategien bei Bedarf an und wiederholen Sie die Implementierung, um die fortlaufende Kostenoptimierung zu gewährleisten.

10 **Erfolge messen und feiern**
Legen Sie KPIs fest, um die Effektivität und Wirksamkeit der FinOps-Strategie zu messen. Verfolgen Sie regelmäßig den Fortschritt anhand von OKRs und KPIs und feiern Sie Meilensteine und Erfolge, um die Motivation der Teams aufrechtzuerhalten.

Fazit

FinOps hilft Unternehmen, Budgetüberschreitungen zu reduzieren, die Kontrolle über Cloud-Ausgaben zurückzugewinnen und den Nutzen von Cloud-Transformationen zu maximieren. Es fördert eine Kultur der Kostenoptimierung und Verantwortung. Durch die Einführung des FinOps Frameworks können Unternehmen ihre Cloud-Kostenmanagement-Strategien im Laufe der Zeit dynamisch weiterentwickeln, um ihre Geschäftsziele auf lange Sicht zu erreichen.

ABB. 2.3: ZEHN SCHRITTE ZUR EINFÜHRUNG VON FINOPS

Warum es an der Zeit ist, Consulting neu zu denken

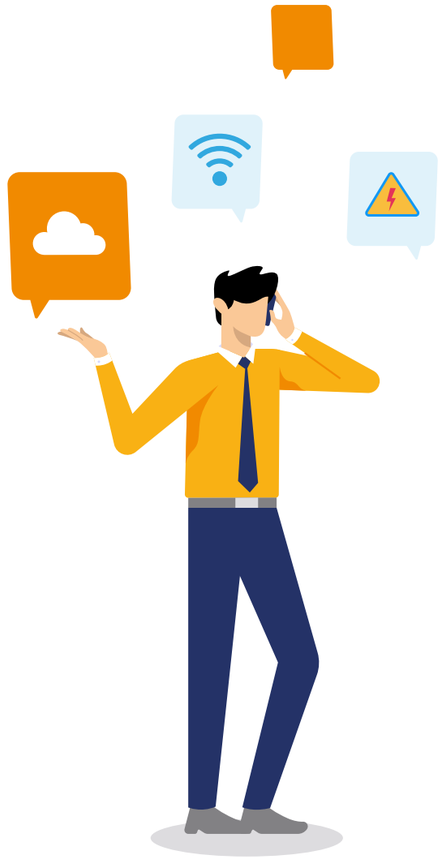
Von Thilo Mundt

Wenn man als Consultant eines Technologie-Unternehmens seinen Kunden sagt, dass Technologie beim digitalen Wandel nicht der entscheidende Punkt ist, dann scheint irgendetwas nicht zu stimmen. Was sollte es sonst sein? Die Antwort auf diese Frage klingt vielleicht ungewöhnlich – aber wir leben in ungewöhnlichen Zeiten.

Genau genommen leben wir in revolutionären Zeiten. Obwohl es fast schon ein Klischee ist, wenn man von der „digitalen Revolution“ spricht, hat dieser Begriff seine Berechtigung. Wir sind zum Beispiel kein bisschen verwundert, wenn große Industriekonzerne von Internet-Start-ups vor sich her getrieben werden. Und gleichzeitig ist uns gar nicht bewusst, dass diese Erschütterungen – wie bei Revolutionen üblich – sehr tief gehen.

Um sich vor Augen zu führen, wie tiefgreifend der Wandel tatsächlich ist, reicht ein kleines Gedankenexperiment: Man muss sich die Welt nur ohne digitale Technologien vorstellen. Kein Internet, kein Smartphone, kein Navi. Tatsächlich würde fast gar nichts mehr funktionieren, weil digitale Systeme heute überall sind. Technologisch leben wir längst im digitalen Zeitalter. Die Frage ist, ob wir dort auch in unseren Köpfen angekommen sind.

„Kreativität, Agilität und Selbstverwirklichung werden zu bestimmenden Faktoren unserer Arbeit.“



Die Veränderungen gehen tief

Man ist leicht versucht, diese Frage zu unterschätzen. Wir haben schließlich überhaupt kein Problem damit, digitale Werkzeuge zu nutzen. Im Alltag ist uns der Umgang damit so in Fleisch und Blut übergegangen, dass wir gar nicht mehr darüber nachdenken, wie viel Technologie in den Dingen steckt. Und gleichzeitig fällt auch nicht weiter auf, wie schnell sich die Welt verändert hat und wie folgenreich die Änderungen sind.

Manchmal fällt es aber doch auf – und zwar immer da, wo dieser Wandel nicht nur passiert, sondern aktiv mitgestaltet wird. Wo Veränderungen Althergebrachtes infrage stellen und wo man sich auf bisher unbekanntes Terrain vorwagt. Genau das ist aber die Situation, in der sich Unternehmen heute befinden. Der digitale Wandel ist in vollem Gang, und mit den neuen technologischen Möglichkeiten werden auch die Karten komplett neu gemischt.

Big Data, künstliche Intelligenz, das Internet der Dinge – all dies eröffnet Unternehmen vollkommen neue Geschäftschancen. Das bedeutet aber zugleich, dass man mit Veränderungen konfrontiert wird, die tief in die Substanz gehen. Digitale Lösungen sind kein Upgrade im klassischen Sinn. Mit ihnen halten neue Arbeitskonzepte Einzug in die Unternehmen. Kreativität, Agilität und Selbstverwirklichung werden zu bestimmenden Faktoren unserer Arbeit. Und das wiederum hat enorme Auswirkungen auf die gesamte Organisation und die Unternehmenskultur.

Außerdem sorgen derart tiefgreifende Veränderungen auch für Verunsicherung. Und diese Verunsicherung kann ganze Projekte zum Scheitern bringen, vor allem, wenn man nach dem Motto vorgeht: Technologie ist alles, und alles andere kommt von selbst. Technologische Entwicklungen treiben den digitalen Wandel an – sie sind aber kein Selbstzweck. Technologie muss den Menschen dienen, die sie einsetzen. Die Antwort auf die eingangs gestellte Frage, was das Entscheidende beim digitalen Wandel eigentlich ist, lautet also: Es sind die Menschen.

„The Power of People“

Wer von dieser Antwort enttäuscht ist oder denkt, dass sich das von selbst versteht, wird vielleicht überrascht sein zu lesen, dass mehr als zwei Drittel aller Digitalisierungsprojekte in Teilen oder komplett scheitern, weil sie genau diesen Aspekt nicht angemessen berücksichtigen. Dass man die Menschen mitnehmen muss, ist viel zu oft ein reines Lippenbekenntnis. Mehr noch: Es ist der falsche Ansatz. Denn es geht nicht darum, die Menschen „mitzunehmen“. Das unterstellt nämlich, dass sie keine aktive Rolle spielen.

Das Gegenteil ist der Fall: Es sind die Menschen in den Unternehmen, die den digitalen Wandel vollziehen. Ihre Kreativität und ihre Leidenschaft machen die digitalen Werkzeuge überhaupt erst stark. Und natürlich ist auch die Verunsicherung ein zutiefst menschlicher Aspekt. Viele fühlen sich überfordert oder haben sogar Angst davor, sich in einem neuen Arbeitsumfeld nicht mehr zurechtzufinden. Wenn die digitale Transformation erfolgreich sein soll, darf man diese Ängste nicht kleinreden oder gar ignorieren.

Es ist mithin offensichtlich, dass der technologische Wandel Teil eines größeren Zusammenhangs ist. Technologie und neue Business-Modelle können nur funktionieren, wenn man sich der kulturellen Erschütterung bewusst wird, die damit einhergeht. Zum ersten Mal haben es Unternehmen mit einer Transformation zu tun, die nicht nur Technologien, sondern auch die Organisationsstruktur und das Mindset aller Mitarbeitenden betrifft. Erfahren diese beiden Aspekte im Rahmen der Transformation keine Veränderung, kann sie nicht gelingen oder zumindest nicht ihr volles Potenzial entfalten.

Womit zugleich eine der zentralen Herausforderungen bei digitalen Transformationsprojekten benannt ist: Man muss die Menschen inspirieren. Das ist nicht trivial, denn immerhin geht es um tiefgreifende Veränderungen. Hierarchien werden aufgebrochen, Altbekanntes wird über den Haufen geworfen, viele werden aus ihrer Komfortzone herausmüssen. Aber es gibt nicht nur Widerstände: Man kann sich auch darauf verlassen, dass Menschen neugierig sind und das Bedürfnis haben, sich persönlich an einer wichtigen und zukunftsweisenden Sache zu beteiligen.

Eine neue Kultur des Wandels

Natürlich spielt auch Technologie eine wichtige Rolle. Letztendlich ist sie die Ursache für die Neubewertung des menschlichen Aspekts. Technologie bildet den Rahmen für die Freisetzung und Förderung kreativer Arbeit. Sie ermöglicht es, orts- und zeitunabhängig zu sein, und schafft damit unausweichlich Freiräume für mehr Selbstverantwortung. Doch gerade an dieser Stelle offenbart sich die kulturelle Erschütterung. Es gibt große Widerstände in klassischen Hierarchien, wenn es darum geht, selbstverantwortliches Arbeiten zuzulassen. Und es ist umgekehrt nicht möglich, Selbstverantwortung von oben zu verordnen.

Klassische Consulting-Ansätze, die sich projektbezogen auf die Implementierung von neuen Technologien und die Schulung der Anwender konzentrieren, stoßen hier an ihre Grenzen. Der digitale Wandel ist nicht einfach nur ein zusätzliches Projekt oder ein Problem, das es zu lösen gilt. Er ist das, was mit allen Unternehmen passiert. So wie auch alle Unternehmen irgendwann elektrifiziert wurden. Das heißt nicht, dass sich ab sofort jeder neu erfinden muss. Es geht vielmehr darum, Unternehmen dabei zu helfen, sich selbst neu zu entdecken.

Und das bedeutet auch, dass man Consulting neu denken muss. Die digitale Transformation der Unternehmen erfordert ein ganzheitliches „Customer Strategy Management“, in dem Technologie, ein motivierendes und emotionalisierendes Zukunftsbild, die Weiterentwicklung der eigenen Geschäftsmodelle und der kulturelle Wandel ineinandergreifen. Für eine erfolgreiche Transformation ist die Orchestrierung dieser vier Aspekte entscheidend. Notwendige Voraussetzung dabei ist, dass die gesamte Organisationsstruktur die beteiligten Menschen dabei unterstützt, ihre Kreativität und ihre besonderen Begabungen zur Entfaltung zu bringen.

Auch die Rolle von Consultants verändert sich dabei fundamental. Ihre Aufgabe besteht nicht primär darin, technologische oder organisatorische Veränderungen zu implementieren. Consultants zeigen Wege auf, wie man die Veränderung selbst zu einem integralen Bestandteil der Unternehmenskultur macht. Gleichzeitig müssen sie sicherstellen, dass keine falschen Erwartungen geschürt und nichts unter den Teppich gekehrt wird. Klar ist, dass der digitale Wandel in vielerlei Hinsicht auch ein schmerzhafter Prozess sein wird. Das ist das Wesensmerkmal aller tiefgreifenden Veränderungen. Aber wenn man es schafft, den beteiligten Menschen plausibel zu machen, warum sich diese Anstrengung lohnt, wird man überrascht sein, wie viel kreative Energie man damit freisetzt.

„Es geht darum, Unternehmen dabei zu helfen, sich selbst neu zu entdecken.“

Edge Computing ist ein Enabler für Echtzeit, Datenschutz und Nachhaltigkeit

Interview mit Benjamin Springub und Dr. Stefan Schnitter

Dr. Stefan Schnitter: Könnten Sie erklären, was unter „Edge Computing“ oder kurz „Edge“ zu verstehen ist und warum es für Geschäftskunden relevant ist bzw. relevant wird?

Benjamin Springub: „Edge Computing“ bezieht sich auf eine verteilte Computing- und Netzwerkstrategie, bei der Datenverarbeitung und -analyse nahe dem Ort erfolgen, an dem die Daten erzeugt werden, also am „Rand“ („edge“) des Netzwerks. Dies ist ein Gegensatz zum traditionellen Cloud-Computing-Modell, bei dem Daten über große Entfernungen zu zentralen Datenzentren übertragen werden. Besonders relevant ist Edge Computing beispielsweise für das Internet der Dinge (IoT), bei dem viele Geräte kontinuierlich Daten erzeugen. Mit Edge Computing können diese Daten effizienter verarbeitet werden, wodurch die Leistung und Funktionalität von IoT-Systemen verbessert wird.

Edge Computing bietet verschiedene Vorteile, die für Geschäftskunden von hoher Relevanz sind. Ein bedeutender Aspekt ist die reduzierte Latenzzeit.

Dies ermöglicht eine Echtzeitverarbeitung von Daten, was für Anwendungen wie selbstfahrende Autos, industrielle Automatisierung oder Telemedizin besonders wichtig ist. Ein weiterer Aspekt ist die Bandbreiteneinsparung. Durch die Verarbeitung großer Datenmengen an der Edge werden Bandbreitenanforderungen reduziert, was in Szenarien mit hohem Datenaufkommen wie etwa bei Videoüberwachungssystemen eine zentrale Rolle spielt.

Weiterhin ermöglicht Edge Computing eine erhöhte Datensicherheit und Privatsphäre. Sensible Daten werden direkt an der Edge verarbeitet, was das Risiko von Datenschutzverletzungen bei Übertragungen über das Core-Netzwerk verringert. Es werden weniger Daten an einem Punkt gesammelt, was eine vollständige Erfassung erschwert. Sensible Daten können zudem vor der Übertragung verschlüsselt werden.

Ein letzter entscheidender Vorteil von Edge Computing ist die verbesserte Verfügbarkeit. Bei Ausfällen oder Verbindungsproblemen zum Core-Netzwerk können Edge-Anwendungen, die keine Verbindung zum Core-Netzwerk benötigen, ohne Einschränkung weiterarbeiten. Das ermöglicht Unternehmen eine höhere Ausfallsicherheit, selbst wenn das Core-Netzwerk vorübergehend nicht erreichbar ist.

Dr. Stefan Schnitter: Gibt es besondere „Edge“-Projekte, auf die Sie gespannt sind oder die Sie in der Zukunft realisieren möchten?

Benjamin Springub: Ich finde generell Projekte spannend, die das Potenzial von Edge Computing in den Bereichen 5G, IoT und Künstliche Intelligenz (KI) weiter ausschöpfen. Diese Technologien könnten von Edge Computing stark profitieren, da sie oft eine schnelle Datenverarbeitung erfordern, die durch Reduzierung der Latenzzeit bei Edge Computing erreicht wird. Es wird auch interessant sein zu sehen, wie Edge Computing dazu beiträgt, die digitale Souveränität und Datenschutzbestimmungen in Europa zu stärken, da Daten lokal verarbeitet und gespeichert werden können. Damit beschäftigt sich auch das IPCEI CIS (Important Project of Common European Interest zu Cloud-Infrastruktur und Services, auf Deutsch “wichtiges Vorhaben von gemeinsamem europäischem Interesse im Cloud Umfeld“). Ein IPCEI ist ein Mechanismus, mit dem die Europäische Union innovative Projekte fördert, die einen erheblichen Einfluss auf die europäische Wirtschaft haben können. Und im speziellen Fall des IPCEI CIS sitzt neben anderen europäischen Telekommunikations- und Industriepartnern auch die Telekom in Deutschland in den Startlöchern, ein Edge Cloud Continuum in Europa aufzubauen.

Spannend ist auch, dass mit Edge Computing und dem IPCEI CIS ein Beitrag zum „Green Deal“ geleistet werden kann, da die Verarbeitung von Daten zunehmend am Ort der Entstehung erfolgt und so weitere Energieeinsparpotenziale erzielt werden können.

Dr. Stefan Schnitter: Welche technologischen Herausforderungen sind mit der Implementierung von „Edge Computing“ verbunden und wie können diese bewältigt werden?

Benjamin Springub: Edge Computing erfordert oft komplexere Netzwerkarchitekturen und kann in erster Linie zu Herausforderungen bei der Datenkonsistenz führen, da Daten an verschiedenen Orten erzeugt und verarbeitet werden. Lösungen können die Implementierung von Protokollen für Datenkonsistenz und Synchronisierung beinhalten. Damit einher geht auch die Verwaltung und Wartung komplexer Infrastruktur, da die Verteilung von Anwendungen und Daten über eine Vielzahl von Edge-Geräten die Netzwerkverwaltung verkomplizieren. Lösungen können den Einsatz von Automatisierung und Machine Learning umfassen.

Dr. Stefan Schnitter: Welche sonstigen, nichttechnologischen Herausforderungen sehen Sie bei der Einführung von Edge?

Benjamin Springub: Ich sehe da in erster Linie die Kosten für die Anschaffung, Installation, Skalierbarkeit und Wartung spezieller Computing-Hardware an den Edge-Standorten. Aber auch Kosten für Mitarbeiterschulungen und Fachpersonal sind nicht zu vernachlässigen.

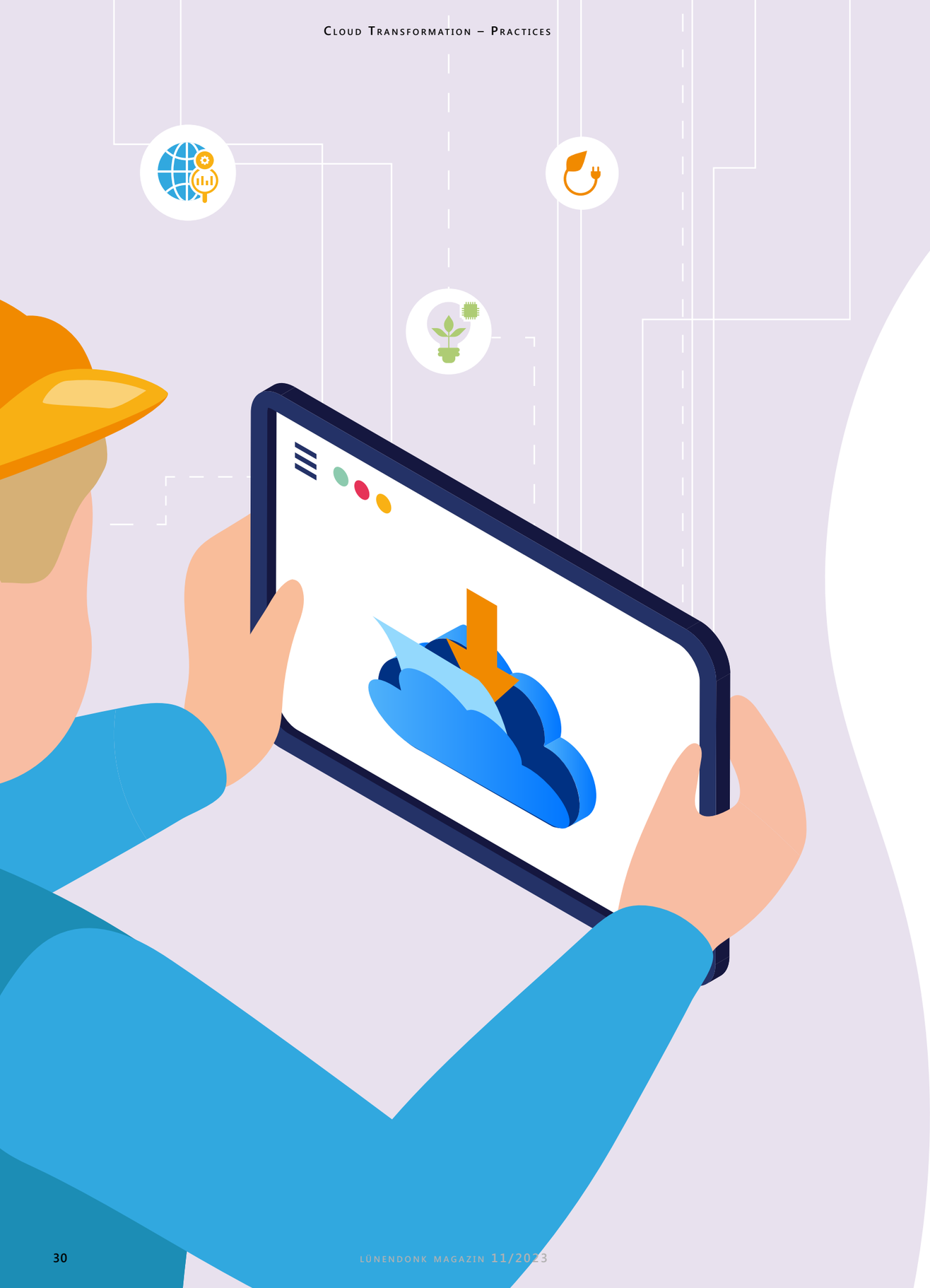
Dr. Stefan Schnitter: Wie sehen Sie die Zukunft von Edge Computing und welche Kunden können besonders davon profitieren?

Benjamin Springub: Ich erwarte, dass Edge Computing in den kommenden Jahren weiterwachsen und eine immer größere Rolle in vielen Branchen spielen wird.

Unsere Health-Kunden, unter anderem Krankenhäuser und andere medizinische Einrichtungen, können Edge Computing nutzen, um Patientendaten in Echtzeit zu verarbeiten und schnellere, präzisere Diagnosen zu ermöglichen. Unsere Kunden aus der Logistikbranche können in Echtzeit Verkehrsinformationen verarbeiten, um die Effizienz ihrer Lieferketten zu verbessern. Energie- und Versorgungsunternehmen können Edge Computing wiederum nutzen, um Echtzeitdaten zu sammeln und so den Energieverbrauch zu optimieren oder spezielle Tarife anzubieten.

Dr. Stefan Schnitter: Ist „Edge Computing“ insbesondere für größere Unternehmen relevant oder kann auch der Mittelstand davon profitieren?

Benjamin Springub: Ich sehe Edge Computing auch im Mittelstand. Im Einzelhandel zum Beispiel könnten mit Echtzeitanalyse personalisierte Einkaufserlebnisse geboten werden. Durch die rasche Auswertung von Daten können Unternehmen besser Rückschlüsse ziehen und wettbewerbsfähig bleiben. Richtig ist aber, dass Edge Computing im Status quo mehr Akzeptanz und Nachfrage von größeren Kunden findet.



Dr. Stefan Schnitter: Viele Unternehmen verknüpfen immer stärker Digitalisierung und Nachhaltigkeit. Wie hängen aus Ihrer Sicht Edge und Nachhaltigkeit zusammen?

Benjamin Springub: Wie bereits erwähnt, sehe ich einen großen Vorteil bei der Energieeffizienz, da Daten lokal verarbeitet werden und so der Energieverbrauch für die Datenübertragung reduziert wird, was wiederum zu einer geringeren CO_2-Belastung führt.

Da Daten schneller verarbeitet werden, können in der industriellen Verarbeitung Prozesse optimiert und Ressourcen effizienter eingesetzt werden. Ein Beispiel ist hier Predictive Maintenance, was Materialverschwendung vorbeugt und die Lebensdauer von Geräten verlängert.

Auch kann der Einsatz von Edge in einer Smart City u.a. den Verkehr optimieren, indem zum Beispiel eine intelligente Ampelschaltung zur Vermeidung von Stau eingesetzt wird. Aber es geht noch weiter: Durch die intelligente Vernetzung und Kommunikation verschiedener Geräte kann zum Beispiel bei einem Feuerwehreinsatz die Einsatzleitung der Feuerwehr deutlich schneller die benötigten Ressourcen zur Brandbekämpfung abschätzen.

Es ist aber auch zu beachten, dass Edge Computing geänderte Herausforderungen in Bezug auf Nachhaltigkeit mit sich bringen kann. Durch angepasste notwendige Hardware für die Edge müssen Strategien für eine umweltfreundliche Herstellung, Nutzung und Entsorgung dieser Geräte entwickelt werden. Zudem gibt es an den Edge-Standorten Herausforderungen hinsichtlich der Kühlung und Wartbarkeit, die an großen Core-Standorten deutlich einfacher umzusetzen sind.

Dr. Stefan Schnitter: Welchen Rat würden Sie Unternehmen geben, die darüber nachdenken, Edge Computing in ihre Abläufe zu integrieren?

Benjamin Springub: Die wichtigsten Schlagworte sind „Planung“ und „Strategie“. Zuallererst sollte eine Bedarfsanalyse erfolgen. Unternehmen sollten also erst mal erheben, wo im Unternehmen Daten erzeugt werden und der Einsatz einer Edge-Infrastruktur sinnvoll sein könnte. In einer Kosten-Nutzen-Analyse sollten die voraussichtlichen Kosten für Hardware, Software, Installation, Wartung und Schulung gegen die zu erwarteten Vorteile wie verbesserte Effizienz und bessere Datenkontrolle abgewogen werden. Dies kann zum Beispiel in einem kleineren Pilotprojekt evaluiert werden. Für die Umsetzung sollten Unternehmen auf Anbieter setzen, die nicht nur die technische Expertise, sondern auch langjährige Erfahrung in der Branche haben.

Dr. Stefan Schnitter: Vielen Dank für das Gespräch.

Erfolgreiche Cloud-Migration: Die Applikation steht im Mittelpunkt

Von Marcus Neumann

Der Nutzen der IT steckt in den Anwendungen. Das gilt auch für Cloud-basierte IT. Cloud-Transformation sollte deshalb immer die Applikationen in den Mittelpunkt stellen. Agiles Vorgehen in kleinen Schritten und konsequente Governance sind die weiteren Erfolgsfaktoren.

Für IT- und Business-Verantwortliche bringt das wachsende Angebot an leistungsfähigen, hoch skalierbaren Cloud-Infrastrukturen neue Chancen, aber auch Herausforderungen mit sich. Denn zum einen ist der Markt immer schwerer zu überschauen, zum anderen verstellen die zahllosen neuen Möglichkeiten in der Cloud nicht selten den Blick auf die eigene Anwendungslandschaft mit ihren Besonderheiten. Verantwortliche für Cloud-Projekte sollten daher von Anfang an den Fokus der Transformation auf die Anwendungen richten. Nur so können sie den maximalen Nutzen der Cloud für ihr Unternehmen erreichen.

Agiles Vorgehen sorgt für schnelle Erfolge

Die Erfahrung zeigt: Für eine erfolgreiche Cloud-Transformation empfiehlt sich ein applikationsbasiertes Vorgehen in kleinen Schritten: von der Analyse der bestehenden Anwendungen über die Definition individueller Transformationsszenarien bis zur erfolgreichen Umsetzung. Mit agilen Methoden können Unternehmen dabei einzelne Anwendungen priorisiert transformieren, um Quick Wins zu realisieren, und gleichzeitig sicherstellen, dass für jede Anwendung der optimale Transformationspfad gefunden wird. Dabei müssen alle Beteiligten sich für jede einzelne Anwendung klarmachen, wo sie stehen und wohin sie wollen.

Das ist eine Herausforderung, deren Umfang oft unterschätzt wird. Schließlich gibt es in vielen Unternehmen und Behörden eine drei- bis vierstellige Anzahl von Anwendungen, die sich in vielerlei Hinsicht unterscheiden: Einige sind gerade erst implementiert, andere laufen seit Jahrzehnten unverändert. Wieder andere werden permanent überarbeitet, obwohl sie kaum jemand nutzt. Um alle Anwendungen nach dem jeweils besten „Fahrplan“ in die Cloud zu bringen, braucht es eine konsequente Governance, also die Steuerung und Verwaltung der Rahmenbedingungen für eine Cloud-Nutzung mit Unterstützung durch Cloud-Experten, die auch die Business-Anforderungen des Unternehmens verstehen.

Jede Applikation im Zusammenhang betrachten

Die Optionen für die Transformation sind vielfältig und ändern sich stetig, sodass oft selbst gestandene IT-Entscheider mit den vielen Optionen nichts anzufangen wissen und falsche Entscheidungen treffen. Anwendungen nur als „Workload“ im Hinblick auf den Bedarf an CPU-, RAM- und Speicherressourcen zu betrachten bringt wenig. Genau das aber geschieht häufig, wenn Cloud-Anbieter und Berater sich vor allem auf die IT-Infrastruktur konzentrieren. Die Praxiserfahrung von Materna aus vielen Cloud-Projekten mit Kunden zeigt: Jede Applikation sollte im Zusammenhang gesehen werden.

An erster Stelle sollte dabei die Frage nach dem Nutzen stehen. Darüber hinaus bieten sich mehrere Hundert Einzelkriterien in unterschiedlichen Kategorien an, um die Transformationsbedürftigkeit und -fähigkeit von Anwendungen zu beurteilen. Technische Daten, Workflows und Geschäftsanforderungen spielen hier ebenso eine Rolle wie die Klassifizierung nach Sicherheitsstufen, Nachhaltigkeitsaspekten, wie etwa der Energiebedarf einzelner Applikationen, oder Datenschutzvorgaben. Nicht zu vergessen: die Abhängigkeiten zwischen Anwendungen.

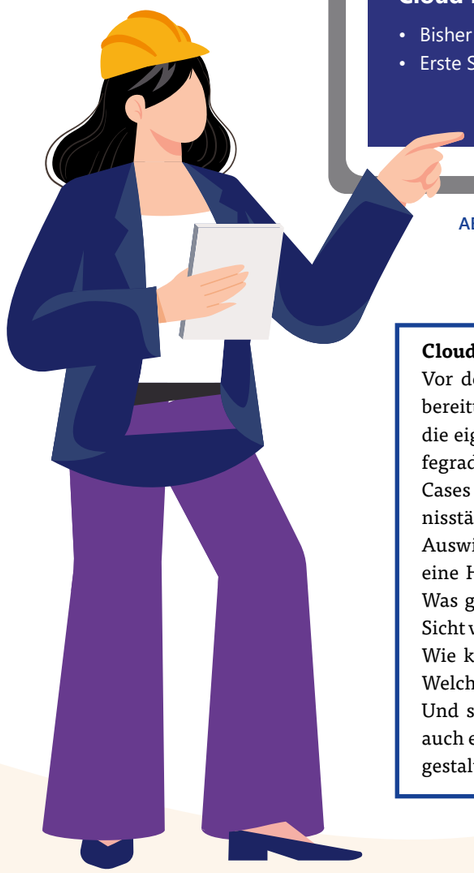


ABB. 3.1: QUELLE: MATERNA

Cloudification – so gehen wir gemeinsam vor
Vor der Reise in die Cloud ist eine gute Vorbereitung wichtig. Dazu gehören zum Beispiel die eigene Positionsbestimmung im Cloud-Reifegrad und die Erstellung relevanter Business Cases für die Cloud. Unterschiedliche Kenntnisstände zu Cloud-Technologien und ihre Auswirkungen zwischen Abteilungen stellen eine Herausforderung bei der Umsetzung dar. Was genau bedeutet der Weg in die Cloud aus Sicht von Security, Governance und Compliance? Wie kann ein Cloud-Framework dabei helfen? Welche Auswirkungen hat das auf den Betrieb? Und schließlich bringt die Reise in die Cloud auch einen Kulturwandel mit sich, den Sie aktiv gestalten müssen.

Materna hilft, diese Zusammenhänge und den Nutzen zu erkennen: auf der Basis jahrzehntelanger Erfahrung als IT-Dienstleister sowie als Cloud-Pionier der ersten Stunde und mithilfe eines standardisierten Verfahrens, das Hunderte Einzelkriterien prüft, um für jede Applikation das optimale Transformationsszenario zu finden.

Analysen automatisieren

Angesichts der Vielzahl von Anwendungen in den meisten Unternehmen empfiehlt es sich, die Analyse der Applikationen so standardisiert und automatisiert wie möglich vorzunehmen. Dabei helfen spezielle Discovery-Tools. Sie werden teilweise kostenfrei von den Cloud-Providern bereitgestellt. Allerdings sind sie zumeist nur auf die infrastrukturspezifischen Details ausgerichtet. Um die vorhandenen Anwendungen so effizient und effektiv wie möglich zu machen, empfiehlt sich darüber hinaus der Einsatz von bewährten IT-Service-Management-Werkzeugen.

Cloud Transformation – Practices

Je nach Bedarf und Compliance-Anforderung des Unternehmens analysieren sie die Anwendungslandschaft des Kunden, scannen Netzwerke und untersuchen die Abhängigkeiten: Welche Anwendungen kommunizieren miteinander? Auf welchem Weg, wie oft und wann? Welche Informationen werden ausgetauscht und in welchen Formaten? Am Ende dieser Analyse steht eine detaillierte Übersicht von Empfehlungen, welche Anwendung wie und wann transformiert werden sollte. Dafür bietet sich die Zuordnung zu vordefinierten Transformationsszenarien an (Siehe Abb. 3.2).

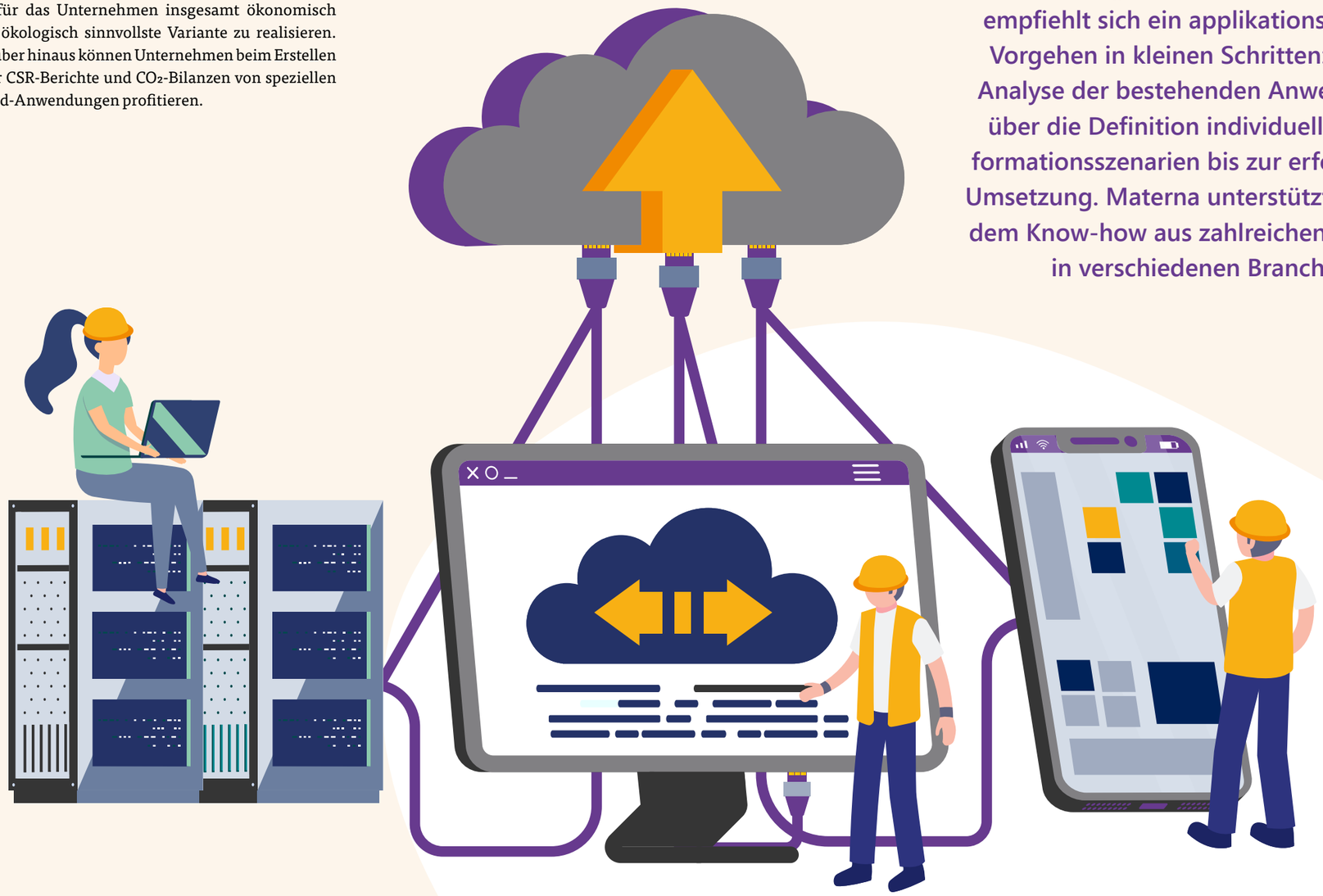
Das Know-how in der Identifikation von Anwendungen für unterschiedliche Transformationsszenarien entscheidet mit darüber, wie schnell und zuverlässig Unternehmen konkrete Quick Wins erreichen, die auf die Unternehmens- und IT-Strategie einzahlen. Dabei hat „quick“ nichts mit „dirty“ zu tun. Und auch nicht mit klein. Wenn zum Beispiel eine modernisierungsbedürftige CRM-Datenbank durch einen entsprechenden Cloud-Service ersetzt wird, kann das gleich mehrere Quick Wins auslösen: die Vereinfachung der zentralisierten Pflege der Kundendaten bei gleichzeitiger Steigerung der Datenqualität. Der wegfallende Aufwand für die Pflege der maroden Datenbank entlastet das wegen des Fachkräftemangels unterbesetzte IT-Team. Und wenn der Cloud-Dienstleister sein Rechenzentrum ausschließlich mit Ökostrom betreibt, verbessert das die CO_2-Bilanz des Unternehmens nachhaltig.

Nachhaltiger dank Cloud

Generell bietet Cloud-Computing Unternehmen die Chance, energie- und ressourceneffizienter zu arbeiten, wie eine Untersuchung des Borderstep-Instituts gezeigt hat. Allerdings kommt es auch hier auf die Betrachtung der einzelnen Anwendung an. Mit modernen Serverless Technologien beispielsweise lässt sich der Energiebedarf wenig genutzter Anwendungen in der Cloud reduzieren. Doch wenn der bislang dafür verwendete Server für andere Anwendungen ohnehin weiterbetrieben werden muss, lohnt sich der Umstieg unterm Strich auch für das Klima nicht.

Auch bei der Frage, wie viel Redundanz eine Unternehmens-IT braucht, wird die Nachhaltigkeit zukünftig eine große Rolle spielen. Denn zum einen muss bei Weitem nicht jede Anwendung rund um die Uhr verfügbar sein. Zum anderen benötigen Applikationen in der Cloud nicht die gleichen Mechanismen wie On-Prem-Installationen, um die Verfügbarkeit zu erhöhen. Die Herausforderung bei der Cloud-Transformation besteht hier darin, unterschiedliche Interessen abzuwägen und mit konsequenter Governance die für das Unternehmen insgesamt ökonomisch und ökologisch sinnvollste Variante zu realisieren. Darüber hinaus können Unternehmen beim Erstellen ihrer CSR-Berichte und CO_2-Bilanzen von speziellen Cloud-Anwendungen profitieren.

Für eine erfolgreiche Cloud-Transformation empfiehlt sich ein applikationsbasiertes Vorgehen in kleinen Schritten: von der Analyse der bestehenden Anwendungen über die Definition individueller Transformationsszenarien bis zur erfolgreichen Umsetzung. Materna unterstützt dabei mit dem Know-how aus zahlreichen Projekten in verschiedenen Branchen.

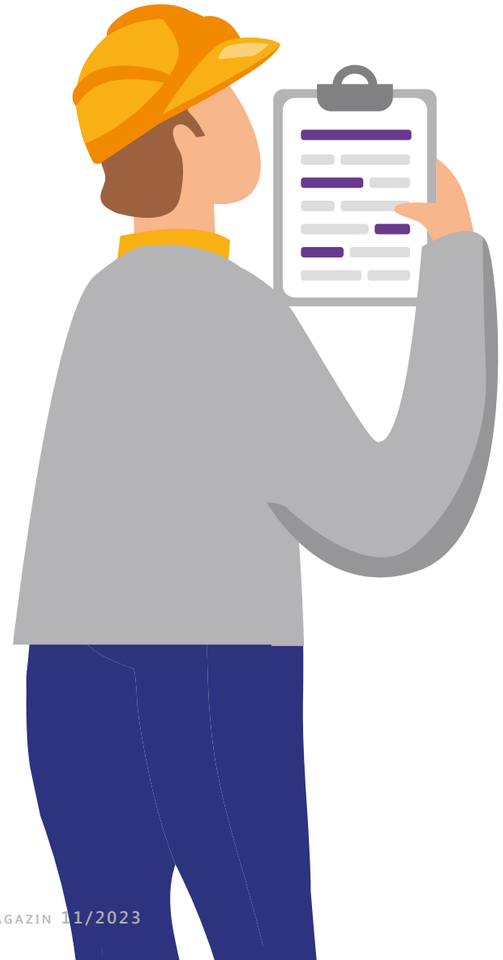


Transformation erfordert IT- und Business-Know-how

Je nach Applikation und Transformationsszenario ergeben sich unterschiedliche Aufgaben, die während der Transformation der jeweiligen Anwendung zu lösen sind. Bei der Migration einer Anwendung in die Cloud kommt es darauf an, den passenden Service für die jeweilige Applikation zu finden. Gibt es ein spezifisches SaaS-Angebot, das alle Anforderungen erfüllt? Auch und gerade im Hinblick auf IT-Security und Compliance? Oder ist der Mehrwert höher, wenn mehrere Services als Paketlösung von einem Anbieter bezogen werden, auch wenn dabei einzelne Funktionen neu hinzuentwickelt werden müssen? Mit dem Wissen über die Möglichkeiten der Cloud allein lassen sich diese Fragen nicht beantworten. Vielmehr ist hier das tiefgreifende Verständnis für Prozesse und Anwendungen von Unternehmen und anderen Organisationen erforderlich, das erfahrene Dienstleister wie Materna mit ihren Anwendungen unterstützen.

IT-Sicherheit und Governance sind Schlüsselfaktoren

Egal, für welches Szenario sich ein Unternehmen bei einer Anwendung entscheidet: Erfolgskritisch ist neben der Auswahl bedarfsgerechter Lösungen die IT-Sicherheit während des gesamten Transformationsprozesses. Dazu gehört auch und gerade die laufende Anpassung der Security-Infrastruktur. Scheinbar geringfügige Veränderungen, wie etwa die Vernetzung eines Vertriebsbüros außerhalb der EU, können hier großen Handlungsbedarf auslösen. Daher gilt für die IT-Security wie für alle anderen Aspekte der digitalen Transformation: Die Veränderung endet nicht, wenn eine Applikation in die Cloud transferiert wurde. Cloud-Transformation bedeutet permanente Veränderung. Und die benötigt vor allem eine strikte Governance, damit bei allen Details, die im Laufe jeder Transformation zu berücksichtigen sind, das Ziel nicht aus den Augen gerät: digitale Geschäftsprozesse, die sich volatilen Märkten anpassen und dem Unternehmen beim Umsetzen seiner Strategie helfen.



Für jede Anwendung das passende Szenario

Unternehmen	Mitarbeiter	Governance	Plattform	Sicherheit	Betrieb
Strategie-Management	Evolution der Kultur	Programm- und Projekt-management	Plattform-architektur	Sicherheits-Governance	Beobachtbarkeit
Portfolio-Management	Transformierende Führung	Nutzer-verwaltung	Datenarchitektur	Sicherheitsansatz	Ereignis-Management (AIOps)
Innovations-Management	Cloud-Expertise	Risiko-management	Plattform-Engineering	Identity und Access Management (IAM)	Vorfalls- u. Problem-Management
Produkt-Management	Belegschafts-Transformation	Cloud-Finanz-Management	Daten-Engineering	Erkennung der Bedrohung	Änderungs- und Versions-Management
Strategische Partnerschaft	Beschleunigung des Wandels	Management d. Anwendungs-Portfolios	Bereitstellung und Orchestrierung	Schwachstellen-Management	Leistungs- u. Kapazitäts-Management
Daten-Monetarisierung	Organisations-design	Daten-Governance	Moderne Anwendungs-entwicklung	Schutz der Infrastruktur	Konfigurations-Management
Business Insights	Ausrichtung d. Organisation	Datenkuratierung	CI/CD	Datenschutz	Patch-Verwaltung
Datenwissen-schaft				Sicherheit der Anwendung	Verfügbarkeits- u. Kontinuitäts-Management
				Reaktion auf Vorfälle	Anwendungs-Management

ABB. 3.2: QUELLE: AWS

Die Kategorisierung der Applikationen in vordefinierte Transformationsszenarien hilft dabei, den Transformationsprozess zu beschleunigen und Ressourcen effizient einzusetzen. Jeder Transformationsbereich wird durch eine Reihe grundlegender Funktionen ermöglicht, die in der Abbildung dargestellt sind. Eine Funktion ist eine organisatorische Fähigkeit, Prozesse zur Bereitstellung von Ressourcen (Mitarbeitende, Technologie und andere materielle oder immaterielle Vermögenswerte) zu nutzen, um ein bestimmtes Ergebnis zu erzielen. Die Funktionen bieten Anleitung anhand von bewährten Methoden, mit denen die Fähigkeit, die Cloud effektiv für die digitale Transformation zu nutzen, verbessert wird. In der Darstellung werden Funktionen in sechs Perspektiven sortiert: Business, Mitarbeiter, Governance, Plattform, Sicherheit und Betriebsablauf.

International wachsen durch Cloud-Technologie – darauf sollten Unternehmen achten

Von Dr. Manuel Audi

Viele Unternehmen denken darüber nach, Cloud-Lösungen für die Skalierung und Internationalisierung ihres Geschäfts einzusetzen. Wir erklären anhand langjähriger Projekterfahrungen am Beispiel der Versicherungsbranche, worauf Unternehmen bei der Internationalisierung mit Cloud-Technologien achten sollten.

Für viele Unternehmen, die in ihren Heimatmärkten erfolgreich agieren, ist internationales Wachstum ein zentraler Faktor ihrer Strategie. Hierbei spielen Cloud-Lösungen eine entscheidende Rolle. Durch ihre Skalierbarkeit und Flexibilität können sie nicht nur Wachstum beschleunigen, sondern auch effizienter gestalten. Sie können die Expansion erleichtern, den Internationalisierungsprozess beschleunigen und sogar die Integration von M&A-Projekten vereinfachen.

Auf dem Weg zur erfolgreichen Internationalisierung müssen Unternehmen verschiedene Herausforderungen bewältigen. Zu diesen gehören das sorgfältige Einbeziehen regionaler Eigenheiten, regulatorische Aspekte, besondere Sicherheitsanforderungen sowie die effektive Integration und Umsetzung der Lösungen. Aus einer Reihe von Projekten, die wir in Zusammenarbeit mit verschiedenen Versicherungsunternehmen durchgeführt haben, möchten wir zehn Thesen ableiten, die unsere Erfahrungen von spezifischen Einzelfällen bis zu allgemein empfohlenen Vorgehensweisen und „Best Practices" zusammenfassen. Die Thesen können Unternehmen daher als Leitfaden dienen, um Herausforderungen zu bewältigen und das volle Potenzial der Cloud-Technologien für ein effizientes und effektives Wachstum auszuschöpfen.

Genaue Planung und Vorbereitung zahlen sich langfristig aus

Ein erfolgreicher Start in die Internationalisierung und Skalierung mit Cloud-Technologien erfordert gründliche Vorbereitungen und eine sorgfältige Projektplanung. Dabei sollten Sie auch von Anfang an lokale Anforderungen und regulatorische Herausforderungen berücksichtigen.

1. Nehmen Sie sich Zeit für gründliche Vorarbeiten:

Jedes Unternehmen ist individuell, ebenso wie die Märkte, in denen es tätig ist. Die Annahme, dass eine zentrale Cloud-basierte Bestandsverwaltungsplattform im europäischen Kontext einfach skaliert, ist schlichtweg falsch. Jedes Land unterliegt eigenen Mechanismen sowie regulatorischen Anforderungen und unterscheidet sich auch auf der Marktseite, beispielsweise bei der Anbindung der Versicherungsprodukte und Vertriebskanäle. Nicht nur Versicherer betreten hier oft Neuland. Für alle gilt: Bei der Internationalisierung und Skalierung kann bereits ein kleines Pilotprojekt eine große Wirkung auf die gesamte Organisation haben. Die Anforderungen zentraler Einheiten sind mit denen dezentraler Landeseinheiten nicht zwangsläufig vereinbar. Prüfen Sie also zunächst sorgfältig Ihre eigenen Geschäftsmodelle und Anforderungen für den Betrieb. Definieren Sie zentrale und dezentrale Aspekte, um Ihre Cloud-Strategie wertorientiert auszurichten, und schaffen Sie eine Arbeitsorganisation, die alle Beteiligten motiviert.

2. Respektieren Sie lokale Anforderungen:

Die internationale Expansion stellt Unternehmen vor viele Herausforderungen, insbesondere wenn es um die Einhaltung lokaler Gesetze und Vorschriften geht. In einigen der von uns begleiteten Projekte war es notwendig, die spezifischen Anforderungen und gesetzlichen Vorgaben jedes Landes zu analysieren und entsprechend zu berücksichtigen. Dieser Prozess bedingte sowohl die Anpassung der Software-Lösung als auch die Definition eines passenden Betriebsmodells, um den unterschiedlichen Marktbedingungen und kulturellen Besonderheiten gerecht zu werden. Versicherungsangebote wirken oft gleich, variieren jedoch stark von Land zu Land. Dies betrifft die enthaltenen Leistungen, die Transaktionen, Geschäftsvorfälle und auch die Vertriebswege – manchmal digital, manchmal analog. Darüber hinaus müssen vor allem streng regulierte Branchen die verschiedenen europäischen Gesetze beachten, etwa in der Buchhaltung (local GAAP, HGB) und im Meldewesen. Berücksichtigen Sie von Anfang an die lokalen Anforderungen und stellen Sie passende und ausreichende Ressourcen für deren Umsetzung bereit.

Verantwortliche, Partner und Stakeholder eng einbinden

Das Einbinden eines erfahrenen Partners und ein aktives Management der verschiedenen Verantwortlichen und Stakeholder tragen zum Projekterfolg bei:

3. Definieren Sie rechtzeitig die Verantwortlichkeiten:

Bei einer Internationalisierung und Skalierung über Cloud-Technologien sind oft lokale und zentrale IT-Systemanpassungen notwendig. Eine Cloud-basierte Lösung kann Ihnen helfen, bestimmte IT-Ressourcen besser, einfacher und günstiger zu betreiben. Eine sorgfältige Organisation ist jedoch essenziell, um Kostensteigerungen, etwa durch individuellen Ressourcenabruf, zu vermeiden. Sie müssen nicht unbedingt eine ganze FinOps-Abteilung einrichten, doch eine klare Zuweisung von lokalen und zentralen Verantwortlichkeiten ist unerlässlich. So können Sie schnell auf Anforderungen reagieren und den Zugriff auf kostbare Cloud-Ressourcen wertstiftend organisieren.

4. Betreiben Sie aktives Stakeholder-Management:

Bei der Internationalisierung sind viele unterschiedliche Stakeholder involviert. Eine solche Initiative gleicht eher einem Marathon als einem agilen 100-Meter-Sprint. Versicherer sollten die Anforderungen der lokalen Märkte und des Heimatmarktes in Einklang bringen. Dies erfordert eine frühzeitige und kontinuierliche Auseinandersetzung mit den lokalen Geschäftsführern, Vertriebs- und Geschäftspartnern, Regulatoren, Produktgebern und Risikoträgern. Ein aktives Stakeholder-Management hilft, die Bedürfnisse und Anforderungen all dieser verschiedenen Parteien zu berücksichtigen.

Technologische Entscheidungen gewissenhaft treffen

Die Wahl der richtigen Technologie und eine klare Strategie bezüglich vorhandener IT-Infrastruktur sind entscheidend für den Projekterfolg:

5. Binden Sie von Anfang an einen erfahrenen Technologiepartner ein:

Bei der Durchführung eines Projekts dieser Größenordnung zeigt sich die entscheidende Rolle eines technologieerfahrenen und umsetzungsstarken Partners. Ein solcher Partner bringt nicht nur das notwendige Know-how für die fachliche Spezifikation und technische Umsetzung mit, sondern versteht auch die strategischen Rahmenbedingungen. In einigen Projekten entwickelten die msg advisors auf der Basis einer Vorstudie ein modulares Betriebs- und Organisationsmodell, das flexibel an lokale Anforderungen angepasst werden kann. Entscheidend hierfür sind die Markteintrittsstrategien, die je nach Land variieren können. Denn es macht einen großen Unterschied, ob Sie eine Niederlassung oder eine Gesellschaft betreiben oder ob Sie ein Unternehmen aufgekauft haben. Flexibilität im Betriebsmodell und in der Plattform ist entscheidend, um den spezifischen Anforderungen des internationalen Geschäfts gerecht zu werden.

6. Wählen Sie die Cloud-Technologie gezielt aus:

Derzeit haben standardisierte Cloud-Lösungen noch nicht die Reife, um international als Cloud-native-Standardplattform eingesetzt zu werden. Hier hilft die Zusammenarbeit mit Technologieanbietern, um die Vorteile einer Cloud-nativen Lösung mit den Vorteilen einer Standardlösung zu kombinieren. Für den Aufbau oder Umzug Ihrer Bestandsverwaltungsplattform empfiehlt sich ein Multi-Cloud-Ansatz. Denken Sie aber auch an Ihre bestehenden On-Premises-Systeme und prüfen Sie, ob und wie sie für eine Internationalisierung nutzbar sind. Auch können unterschiedliche Anforderungen der einzelnen Länder die Entwicklung landesspezifischer Softwarelösungen erfordern.

7. Vergessen Sie nicht die Legacy-IT:

Bei Übernahmen oder Beteiligungen müssen Sie oft mit bestehenden IT-Systemen des lokalen Bestandsgeschäfts umgehen. Überlegen Sie frühzeitig, ob die bestehenden Systeme weiterbetrieben oder auf die Cloud-Plattform migriert werden sollen. Ob Migration auf die Zielplattform, paralleler Betrieb von Zielplattform und Legacy-IT oder sogar der Verkauf der Bestände und die Ablösung der Legacy-IT – alle Optionen haben ihre Vor- und Nachteile, die es zu bewerten gilt. Wichtig ist, dass Sie sich rechtzeitig und umfassend mit dieser Situation auseinandersetzen, um die bestmögliche Entscheidung zu treffen. Eine IT-Due-Diligence-Überprüfung gibt schon während des Unternehmenserwerbs Orientierung.

Auf Standardisierung, Agilität und Einfachheit setzen

Ein erfolgreicher Einsatz von Cloud-Technologien hängt stark ab vom Grad der Standardisierung sowie der Effizienz und Agilität der Implementierungsstrategien:

8. Hinterfragen Sie den Individualisierungsbedarf:

Eine hohe Standardisierung steigert die Effizienz und reduziert Kosten, steht aber oft im Konflikt mit landesspezifischen Bedürfnissen. Internationale Projekte profitieren von vereinheitlichten Strukturen und reduzierten Wartungsaufwänden. Zwingende lokale Anforderungen müssen jedoch berücksichtigt werden. Ein zielgerichtetes Anforderungsmanagement hilft, diese Konflikte zu lösen. Die Praxis zeigt, dass es sinnvoller ist, die Arbeitsweise der Mitarbeitenden an die IT-Plattform anzupassen, anstatt kostspielige Individualisierungen vorzunehmen.

9. Übertreiben Sie es nicht mit agilen Methoden:

Agile Methoden können helfen, Annahmen rasch zu validieren und Anforderungen zügig umzusetzen. Sie sind besonders nützlich in komplexen und unsicheren Bereichen wie internationalen Initiativen. Aber Agilität sollte maßvoll eingesetzt werden. Die Komplexität entsteht aus lokalen und zentralen Interessen und der Koordination zwischen Business und IT. Diese Herausforderungen erfordern sorgfältige Planung und ein transparentes Management von Erwartungen, nicht nur Agilität. Erst wenn Erwartungen abgestimmt, der Scope definiert und agile Strukturen etabliert sind, lassen sich Anforderungen agil umsetzen.

10. Setzen Sie auf Einfachheit:

Leicht zu handhabende Produkte und Prozesse sind besser skalierbar und für den internationalen Einsatz geeignet. Vermeiden Sie unnötige Komplexität. Dies beginnt schon beim Produktdesign, das klare und einfach beherrschbare Differenzierungsmerkmale für den Wettbewerb bieten sollte. Überdenken Sie Ihr Produktportfolio je nach Markt (B2B, B2B2C, B2C) und beachten Sie die Produktlebenszyklen sowie die nachgelagerte Komplexität. Cloud-Technologien können hierbei die Variabilisierung der IT-Ressourcen und Vereinfachung der IT-Prozesse unterstützen.

Die Zukunft der Internationalisierung liegt in der Cloud

Wer Ökosysteme schaffen will, muss auf die Cloud setzen. Doch obwohl Cloud-Lösungen bedeutende Vorteile bieten, garantieren sie noch keinen erfolgreichen globalen Ausbau. Jede Branche und jedes Unternehmen hat spezifische Anforderungen, die bei der Entwicklung und Implementierung von Cloud-Strategien berücksichtigt werden müssen.

Eine erfolgreiche Internationalisierung erfordert eine gründliche Planung, kontinuierliche Anpassung und organisatorische Flexibilität. Dann sollte der erfolgreichen Cloud-Skalierung nichts mehr im Wege stehen.

ABB. 4.1: HANDLUNGSEMPFEHLUNGEN FÜR DIE INTERNATIONALISIERUNG UND SKALIERUNG MIT CLOUD-TECHNOLOGIEN

IT-Sicherheit und Datenschutz haben Priorität

Bei der Nutzung von Cloud-Technologien haben Sicherheit und Datenschutz höchste Priorität. Dies gilt insbesondere bei internationaler Expansion, da die Datenschutzgesetze und -vorschriften von Land zu Land variieren können. Obwohl Cloud-Lösungen in vielen Bereichen eine erhöhte Sicherheit bieten können – beispielsweise durch automatische Updates und aktuellste Sicherheitsmaßnahmen –, liegt das Management der Datensicherheit und die Einhaltung der Datenschutzgesetze stets in der primären Verantwortung des Unternehmens.

Es ist dabei nicht nur entscheidend, dass der ausgewählte Cloud-Anbieter über robuste Sicherheitsprotokolle verfügt, sondern auch, dass er die Compliance-Anforderungen in den Ländern, in denen Sie tätig sind, erfüllt. Von der Datenverschlüsselung, über Zugriffskontrollen bis zu regelmäßigen Sicherheitsaudits – es gibt eine Reihe von Maßnahmen, die berücksichtigt werden sollten. Unser Autor Jens Westphal beleuchtet dieses Thema in seinem Fachartikel auf Seite 54.

Governance ist der Schlüssel zu sicheren und nachhaltigen Cloud-Lösungen

Interview mit Marcus Neumann

Die Sicherheit und Nachhaltigkeit von Cloud-Lösungen werden immer wieder kontrovers diskutiert. Erst recht, wenn es um die Kosten geht. Marcus Neumann erklärt im Interview, wie Governance hilft, Cloud-Lösungen sicher, nachhaltig und wirtschaftlich zu gestalten.

Lünendonk: Herr Neumann, Cloud-Computing gewinnt für Unternehmen in allen Branchen und jeglicher Größe an Bedeutung. Warum tun sich trotzdem noch viele Organisationen so schwer mit dem Umstieg?

Marcus Neumann: Das ist in der Tat ein Phänomen, mit dem auch wir als Berater täglich konfrontiert sind. Meiner Erfahrung nach ist die Herangehensweise nicht immer passend. Unternehmen halten sich gern an die Cloud Adoption Frameworks der Hyperscaler. Tatsächlich sind die gut geeignet, um sich vor Augen zu führen, was man bei der Migration in die Cloud alles bedenken muss. Sie bieten Hilfestellungen, welche Themen wichtig sind, um einen Erfolg zu erzielen. Wie bei vielen Methoden kann man iterativ in kleinen Schritten umsetzen oder bis ins kleinste Detail planen und vorbereiten. Im letzten Fall, der zu häufig vorkommt, entstehen hohe Kosten vor den ersten Erfolgen. Das frustriert.

Lünendonk: Ist es ein Fehler, die vielen Abhängigkeiten in einem Cloud-Projekt frühzeitig zu adressieren?

Marcus Neumann: Nein, es kommt nur darauf an, wie man es macht. Ich vergleiche das gern mit einem Hausbau. Eine gute Planung und ein stabiles Fundament sind wichtig. Aber auch während des Hausbaus können noch Änderungen in der Planung vorgenommen werden: eine Tür etwas versetzen, eine Steckdose hier mehr. Das bringt kein Problem mit der Statik, ermöglicht aber, schneller zu beginnen und flexibler zu sein. Ganz ähnlich ist es bei der Cloud-Migration: Zunächst mal ist es wichtig, sich auf den Nutzen zu fokussieren. Was braucht das Unternehmen wirklich, um schnell einen Nutzen zu generieren? In der Regel ist das nicht die Modernisierung der Archivlösung, sondern eher ein einheitliches Kundenbeziehungsmanagement, eine zentralisierte Fertigungs- und Logistiksteuerung oder eine Cloud-basierte Produktentwicklungsplattform, an der Techniker rund um den Globus und rund um die Uhr arbeiten können. Anwendungen also, die wertschöpfende Prozesse unterstützen. Und zwar besser unterstützen als die bisherige On-Premises-Lösung. Damit heißt es anfangen. Hier lassen sich schnell erste Erfolge erzielen, die dann die Motivation und idealerweise auch die Finanzierung der nächsten Schritte erleichtern.

Lünendonk: Wie lässt sich verhindern, dass einzelne Unternehmensbereiche ihre Lieblingsprojekte pushen und ungeliebte Aufgaben anderen überlassen?

Marcus Neumann: Das ist, wie der Projekterfolg insgesamt, eine Frage der konsequenten Governance. Wir verstehen darunter ein strukturiertes System zur Steuerung von organisatorischen Prozessen. Bezogen auf die Cloud-Transformation geht es um klare Regeln zum Maximieren der organisatorischen Vorteile und Minimieren der mit der Transformation verbundenen Risiken. Insbesondere ist Governance die Grundlage dafür, die Sicherheit von Daten, Anwendungen, Infrastruktur und Menschen in der Unternehmens-IT gewährleisten zu können. Genauso gehört dazu, verbindliche Sicherheitslevel für die unterschiedlichen Daten im Unternehmen festzulegen. Ebenso wie Regeln für das Identitäts- und Zugriffs-Management, Schulungspläne für die Mitarbeitenden und die Organisation von Sicherheitstests und -übungen. Und das sind nur einige der Fragen, die sich allein im Bereich der IT-Sicherheit stellen.

Lünendonk: Beim Thema Sicherheit kollidiert ja oft das Interesse an einer möglichst sicheren IT mit dem Interesse an einer möglichst einfachen Handhabung. Was bedeutet das für die Governance?

Marcus Neumann: Deshalb ist kompetente Governance ja so wichtig. Sie muss sicherstellen, dass immer der Nutzen des Unternehmens als Ganzes im Vordergrund steht. Dazu braucht es Regeln, um beispielsweise die Vertraulichkeit von Daten zu definieren – nicht nur anhand der DSGVO, sondern auch im Hinblick auf den Wert der Daten für das Unternehmen. Diese Regeln zu gestalten, erfordert eine Menge Know-how. Nicht nur technisch, sondern auch organisatorisch in Bezug auf die Unternehmensprozesse. Und es braucht Erfahrung, wie man die Einhaltung der aufgestellten Regeln sicherstellt.

Lünendonk: Welcher Aspekt ist beim Thema Governance am wichtigsten?

Marcus Neumann: Die Dinge im Zusammenhang zu sehen. Governance umfasst ja viele weitere Aufgaben. So etwa das Optimieren der Kosten in der Cloud.

Lünendonk: Wo ist der Zusammenhang mit dem Sicherheitsthema?

Marcus Neumann: In vernetzten Unternehmen ist das Risiko eines Sicherheitsvorfalls nie vollständig auszuschließen. Deshalb müssen Sicherheitsmaßnahmen von vornherein einkalkuliert und geplant werden. Auch in dem Wissen, dass es hundertprozentige Sicherheit nicht gibt. Das gilt im Übrigen nicht nur in der Cloud. Das alte Prinzip „Wir entwickeln erst mal und dann sichern wir die Lösung ab“ funktioniert nicht mehr. Vermeintliche Kostenoptimierung durch Sparen bei den Sicherheitsmaßnahmen muss durch Governance-Regeln ausgeschlossen werden. Denn die Kosten eines Sicherheitsvorfalls können ein Unternehmen ruinieren. Gleichzeitig kann das Herunterfahren einer Anwendung bei einem Sicherheitsvorfall den Schaden minimieren – obwohl es seinerseits Kosten verursacht. Natürlich geht es immer zuerst darum, solche Situationen zu verhindern – beispielsweise durch die konsequente Anwendung von Authentifizierungs- und Autorisierungsanforderungen für den Zugriff auf Anwendungen. Das kann auch mal bedeuten, dass ein Geschäftsführer am Sonntagmorgen nicht mit dem Handy auf eine bestimmte Kennzahl zugreifen kann, wenn er sich in einem unsicheren Hotel-WLAN befindet.

Lünendonk: Auch Nachhaltigkeit ist ein zentrales Thema im Zusammenhang mit der Cloud-Transformation. Eine typische Frage lautet: Wie viele Ressourcen braucht das Unternehmen? Was antworten Sie darauf?

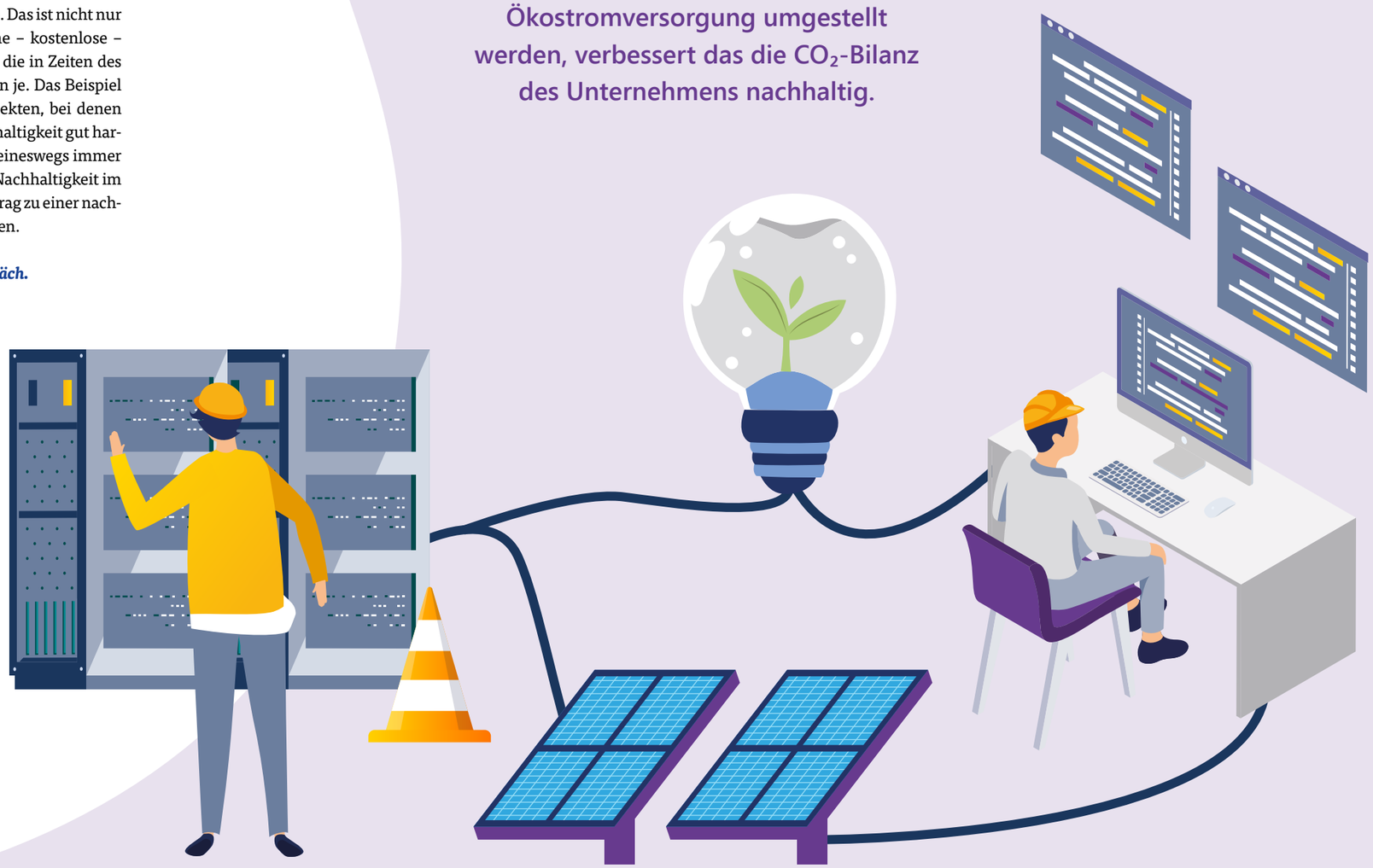
Marcus Neumann: Nicht alles, was Cloud-Provider rund um die Uhr bereitstellen, wird permanent benötigt. Governance sorgt dafür, nur das zu buchen, was auch gebraucht wird. Skalieren, wenn mehr benötigt wird, geht schnell. Und unsere Erfahrung bei Materna zeigt: Häufig lässt sich damit auch eine Menge Geld sparen. Das heißt, ökologische und ökonomische Nachhaltigkeit sind gut vereinbar. Inzwischen bieten die großen Cloud-Provider Tools an, mit denen Unternehmen den CO_2-Fußabdruck ihrer Cloud-Nutzung nicht nur messen, sondern auch dokumentieren können. Das ist vor allem im Hinblick auf die kommende Neuregelung der CSR-Berichtspflicht in der EU von Bedeutung – und unterstützt die Steuerung von Maßnahmen zur Umsetzung der eigenen Nachhaltigkeitsstrategie. Auch Materna bietet hierfür eine explizite Lösung. Ein gemeinsames Angebot mit dem ESG-Software-Pionier VERSO aus München unterstützt Unternehmen, ein zukunftsfähiges Nachhaltigkeitsmanagement aufzubauen – und sich so optimal für die nachhaltige Transformation aufzustellen. Die umfassende Datenerhebung sowie die damit verbundenen internen Prozesse stellen die größte Hürde für Unternehmen bei der Erfüllung der CSR-Berichtspflicht dar. Hier setzt unser Angebot an: Die dezentrale Prozess- und systemübergreifende Datenerhebung durch Entwicklung maßgeschneiderter Software-Lösungen zählt seit mehr als 40 Jahren zu den Kernkompetenzen von Materna. Hinzu kommt die kundenindividuelle Beratung. In Kombination mit der CSR-/ESG-Software von VERSO, die Materna in ihr Portfolio aufgenommen hat, entsteht die optimale Lösung.

Lünendonk: Welche Nachhaltigkeitsmaßnahmen verfolgt Materna?

Marcus Neumann: Wir haben bereits 2022 alle deutschen Standorte von Materna SE auf Ökostrom umgestellt und setzen in unserem Fuhrpark auf Elektromobilität. Viel wichtiger, weil es da um ganz andere Größenordnungen geht, sind unsere Kundenprojekte. Dabei helfen wir Unternehmen, durch Digitalisierung – auch mit Cloud-Anwendungen – ihre Geschäftsprozesse nachhaltiger zu gestalten. Zum Beispiel durch die Umstellung auf Remote Service bei einem Anlagenbauer. Das vermeidet unnötige Fahrten, spart Treibstoff sowie die damit verbundenen Emissionen und schont so die Umwelt. Auch hier gibt es erhebliche ökonomische Vorteile: Weniger Servicefahrzeuge verursachen auch weniger Betriebskosten für Versicherung, Wartung, Reparaturen etc. Die Reisekosten im Field Service sinken ebenfalls. Außerdem freuen sich die Mitarbeitenden über angenehmere Arbeitszeiten und -bedingungen. Sie müssen weniger reisen, können Familie und Beruf besser vereinbaren. Das ist nicht nur sozial nachhaltig, sondern auch eine – kostenlose – Maßnahme zur Mitarbeiterbindung, die in Zeiten des Fachkräftemangels wichtiger ist denn je. Das Beispiel ist nur eines von vielen Kundenprojekten, bei denen ökonomische und ökologische Nachhaltigkeit gut harmonieren. Dabei gilt: Die Cloud ist keineswegs immer die allumfassende Lösung für mehr Nachhaltigkeit im Unternehmen, aber ein wichtiger Beitrag zu einer nachhaltigen Transformation von Prozessen.

Lünendonk: Vielen Dank für das Gespräch.

Cloud-Computing bietet Unternehmen die Chance, energie- und ressourceneffizienter zu arbeiten. Und wenn zudem der Cloud-Dienstleister sein Rechenzentrum mit Ökostrom betreibt oder auch die eigenen Standorte auf Ökostromversorgung umgestellt werden, verbessert das die CO_2-Bilanz des Unternehmens nachhaltig.



Herausforderungen der Cloud-Transformation

Von Mario Zillmann

Die Cloud eröffnet Unternehmen und Behörden den Weg in die digitale Transformation. Je höher jedoch der Cloud-Reifegrad und je stärker die Integration von Cloud-Services in die Wertschöpfung zunimmt, umso mehr Anforderungen an den Betrieb der Cloud-Prozesse ergeben sich. Das gilt nicht nur für Branchen mit großer Regulierungstiefe wie Energieversorger, Finanzdienstleister und den öffentlichen Sektor. Beispielsweise ergibt sich durch die EU-Datenschutz-Grundverordnung (EU-DSGVO) ein grundsätzliches Risiko für Unternehmen und Organisationen, wenn sie Kundendaten in der Public Cloud eines US-amerikanischen Cloud-Anbieters speichern, da der Zugriff US-amerikanischer Behörden auf diese Daten zwar schwierig, aber nicht unmöglich ist.

Cloud-Transformation und Cloud-Security müssen Hand in Hand gehen

Bei der Cloud-Nutzung spielen Sicherheitsanforderungen eine besonders große Rolle, um den Schutz von Daten, Anwendungen und Infrastrukturen zu gewährleisten und potenzielle Sicherheitsrisiken zu minimieren. Während die klassischen (und meist in sich geschlossenen) IT-Infrastrukturen in der Regel gut geschützt sind, ergeben sich mit der Nutzung von IT-Leistungen aus der Cloud neue Angriffsvektoren und damit ein hohes Risiko der Kompromittierung der IT-Systeme und des Diebstahls von sensiblen Daten. Dies ist beispielsweise in produzierenden Unternehmen derzeit ein großes Thema bei der Digitalisierung der Operational Technology (OT), da eine Vielzahl an Hardware-Devices mit der Cloud vernetzt werden und Daten kontinuierlich gesammelt werden. Dies betrifft aber per se digitale Produkte, bei denen Kundendaten erhoben werden, sowie alle anderen Branchen.

Unternehmen im EU-Raum sind gesetzlich verpflichtet, bestimmte Datenschutz- und Sicherheitsstandards einzuhalten. Um ihre Cloud-Systeme und Daten zu schützen, müssen sie daher geeignete Schutzmaßnahmen wie Verschlüsselung oder ein Identity-and-Access-Management implementieren. Für Finanzdienstleister und KRITIS-Branchen ist durch die Regulatorik (BAIT, VAIT, Dora, NIS etc.) die Einführung entsprechender Security-Prozesse und einer klaren Cloud Governance vorgeschrieben. Aufgrund der stark steigenden Cyberbedrohungslage gilt es nun für alle anderen Branchen, bei ihrer Security-Reife nachzuziehen.

Tatsächlich hat sich Cyberkriminalität mit fortschreitender Digitalisierung zu einer der größten Bedrohungen für Unternehmen entwickelt. Laut dem Report „Die Lage der IT-Sicherheit in Deutschland 2022“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist das sogenannte Big Game Hunting, also die Erpressung umsatzstarker Unternehmen mit erbeuteten Daten, stark angestiegen. In der Folge waren nicht nur steigende Lösegeldzahlungen zu beobachten, sondern auch ein deutlicher Anstieg der veröffentlichten Daten von Unternehmen, die keine Zahlung geleistet haben. Weiterhin besorgniserregend ist laut dem BSI auch die Geschwindigkeit und Professionalität der Hackerinnen und Hacker: So hat die Anzahl neuer Schadprogrammvarianten 2022 um rund 116,6 Millionen zugenommen, was es zunehmend erschwert, Cyberangriffe zu entdecken. Immer häufiger kommt es auch zu Ransomware-Attacken. Diese beginnen in der Regel mit einer Phishing-Kampagne und dem Versuch, einen Rechner im Firmennetzwerk zu kompromittieren. Treiber solcher Angriffe sind eine oft nicht ausreichende Absicherung der Netzwerke und Firewalls, die Phishing-Mails in der Regel nicht erkennen.

Cloud-Dienste werden genutzt, aber beim Teilen ihrer Daten sind viele Unternehmen noch vorsichtig

Personenbezogene Daten müssen laut Bundesdatenschutzgesetz (BDSG) und EU-Datenschutz-Grundverordnung (EU-DSGVO) besonders geschützt werden, andernfalls drohen Bußgelder. Gleichzeitig bestehen in der EU weiterhin Vorbehalte respektive eine unklare Rechtslage gegenüber der Datenspeicherung in den Public Clouds der Hyperscaler – vor allem, weil dies den Zugriff US-amerikanischer Behörden auf Unternehmens- und Kundendaten ermöglicht.

Um die Übertragung von Daten an US-amerikanische Public-Cloud-Provider rechtssicher aufzustellen, wurden in der Vergangenheit bereits mehrere Abkommen aufgesetzt. Bereits 2016 wurde jedoch das Safe-Harbour-Abkommen zwischen der EU und den USA als unzureichend bewertet. Auch das Folgeabkommen, der US Privacy Shield, wurde 2020 vom Europäischen Gerichtshof im Zuge des Schrems-II-Urteils als rechtsungültig erklärt. Eine endgültige rechtliche Lösung steht bisher aus.

Diese Situation hat jedoch Auswirkungen auf die Geschwindigkeit der Cloud-Transformation. Tatsächlich schätzt derzeit nur jedes dritte von Lünendonk befragte Unternehmen seine Bereitschaft, Daten in der Cloud zu teilen beziehungsweise in der Public Cloud bereitzustellen, als sehr oder eher hoch ein. Zukünftig rechnen zwar 51 Prozent der Unternehmen mit einer Verbesserung der datenschutzrechtlichen Voraussetzungen, jedoch besteht nach dem Urteil der irischen Datenschutzbehörde gegen Meta aus dem Mai 2023 auch weiterhin eine hohe Unsicherheit aufseiten von Wirtschaft und Behörden.

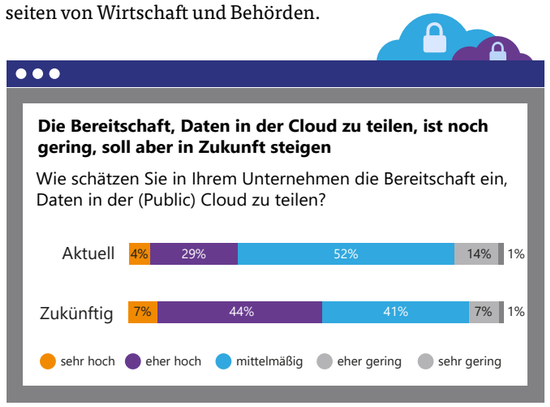


ABB. 5.1: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, SKALA VON 1 =„SEHR GERING“ BIS 5 = „SEHR HOCH“; ALLE TEILNEHMER; N = 119

Cloud-Governance bei Hybrid- und Multi-Cloud-Strategien: Integrierte Security-Orchestrierung ist gefragt

Die meisten Unternehmen verfolgen mit ihrer Cloud-Strategie einen Multi- und Hybrid-Cloud-Ansatz. Da sich mit zunehmender Nutzung multipler und hybrider Cloud-Prozesse neue Angriffsvektoren ergeben, ist es erforderlich, in das Security-Information-and-Event-Management (SIEM) oder in das Identity-and-Access-Management zu investieren, um die bestehenden Unternehmensnetze zu schützen.

Druck, in diesen Bereichen zu investieren, ergibt sich nicht nur durch regulatorische Vorgaben und selbst auferlegte Cloud-Governance-Richtlinien, sondern auch durch die steigende Zahl an professionellen Hackerangriffen. Daher ist es ratsam, die Überwachung der einzelnen Cloud-Services an einer zentralen Stelle (z. B. in einem Security Operations Center) zusammenlaufen zu lassen und eine zentrale Cloud Governance zu etablieren. Ein wichtiges Element einer wirkungsvollen Cloud Governance ist neben dem Aufbau eines zentralen SIEM eine End-to-End-Integration der hybriden Multi-Cloud- und Multi-Provider-Umgebungen in die Security-Prozesse. Eine solche integrierte Security-Orchestrierung ist laut Lünendonk-Research allerdings nur in etwa jedem dritten Unternehmen bereits vorhanden, sodass hier angesichts einer stark steigenden Bedrohungslage und einer zunehmenden Cloud-Nutzung großer Handlungsbedarf besteht.

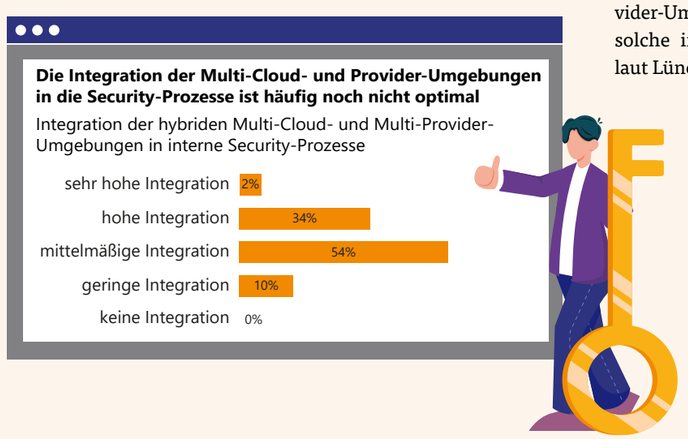


ABB. 5.2: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, SKALA VON 1 =„KEINE INTEGRATION“ BIS 5 = „SEHR HOHE INTEGRATION“; ALLE TEILNEHMER; N = 99

Hybrid- und Multi-Cloud: Die Umsetzung einer Cloud Governance und die Orchestrierung der Cloud-Services sind große Herausforderungen

Eine große Herausforderung ist außerdem die hohe Komplexität bei der Integration (Orchestrierung) der hybriden und multiplen IT-Service-Prozesse. Beispielsweise laufen Geschäftsprozesse zunehmend auf mehreren Deployment-Modellen und verteilt in den Rechenzentren unterschiedlicher Cloud-Anbieter und Managed-Service-Provider, wodurch die Komplexität im IT-Service-Management stark zunimmt. Für 92 Prozent der Befragten ist die Orchestrierung der hybriden und multiplen IT-Service-Prozesse eine große Herausforderung. Dies ist unter anderem auf fehlende Kompetenzen, den Fachkräftemangel und auf generell kleinere IT-Abteilungen zurückzuführen.

69 Prozent der Unternehmen haben bereits hybride beziehungsweise multiple Cloud-Umgebungen implementiert. Die Nutzung von Cloud-Ressourcen bei gleichzeitiger Berücksichtigung von Risk-Management respektive regulatorischen Anforderungen führt unweigerlich zu hybriden und multiplen Strukturen im IT-Betrieb. Die Steuerung solcher Prozesse – vor allem unter dem Aspekt der Cybersecurity – ist eine enorm große Zukunftsaufgabe, aus der sich einige dringende Herausforderungen ergeben (u. a. aufgrund der ab 2023 im Finanzdienstleistungssektor geltenden DORA-Richtlinie).

Eine besonders große Herausforderung ist für 97 Prozent der Unternehmen die Entwicklung und Operationalisierung einer Cloud Governance. Sie soll nachvollziehbare Regeln zur Nutzung von Cloud-Services festlegen. Beispielsweise: Wer darf über den Einsatz der Cloud entscheiden? Wer hat die Übersicht über die genutzten Cloud-Services? Wer darf Zugriffe und Rechte verwalten? Wie und wo werden Daten gespeichert? Ebenso sollte eine Cloud Governance Service Level Agreements (SLAs) regeln – sowohl intern als auch gegenüber externen Providern.

Hybride und multiple Cloud-Umgebungen ziehen eine Vielzahl an neuen Anforderungen nach sich

Nutzen Sie für den Betrieb von Teilen Ihrer Workloads hybride oder multiple Cloud-Umgebungen?

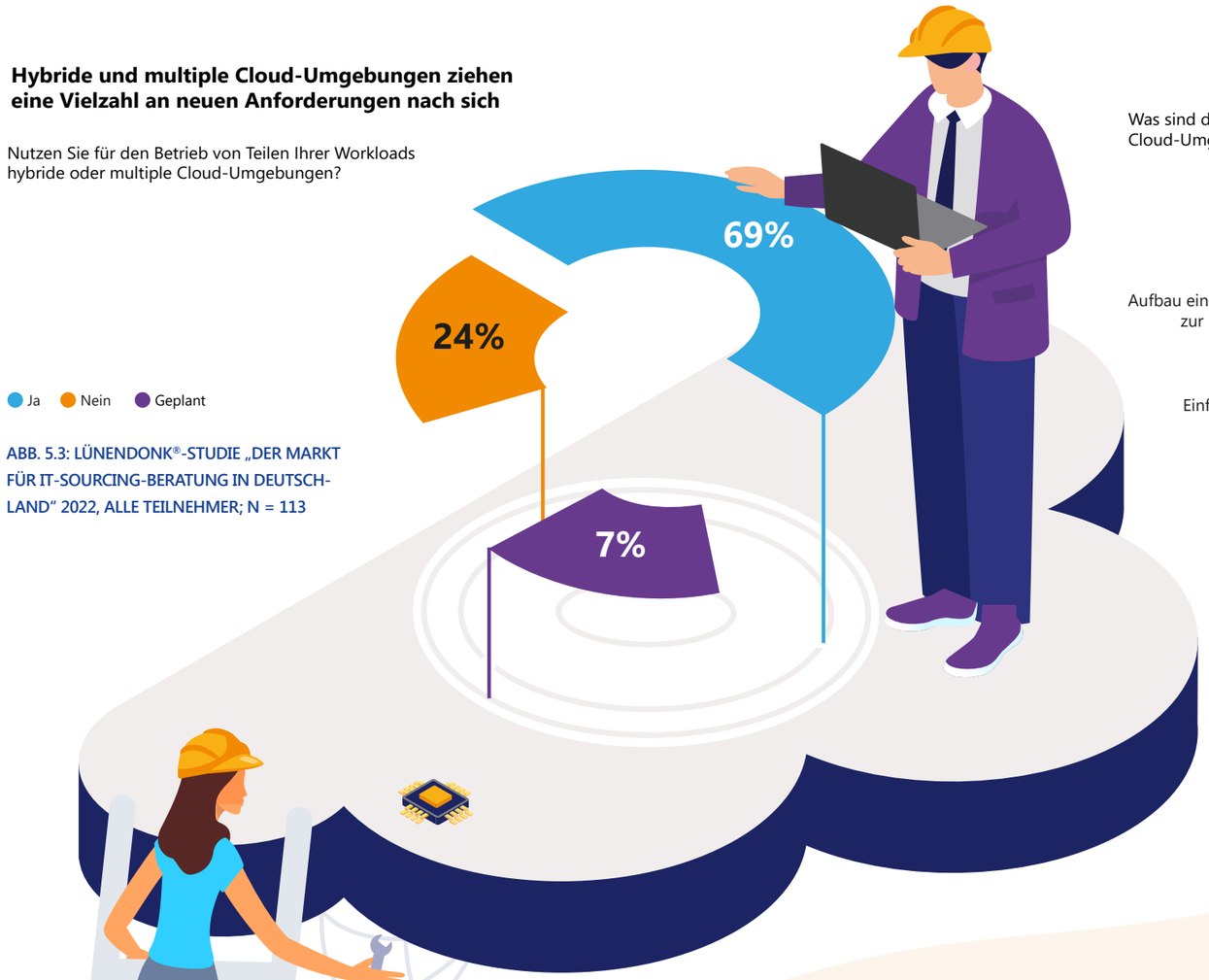


ABB. 5.3: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, ALLE TEILNEHMER; N = 113

Compliance & Security

Was sind die größten Herausforderungen im Management solcher hybriden und multiplen Cloud-Umgebungen?

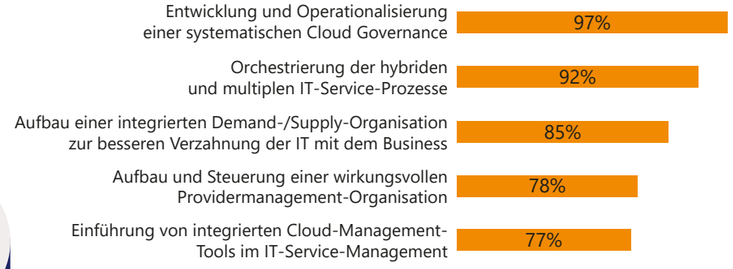


ABB. 5.4: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, SKALA VON 1 =„KEINE HERAUSFORDERUNG“ BIS 5 = „SEHR GROSSE HERAUSFORDERUNG“; ALLE TEILNEHMER; N = 98

Im gleichen Kontext stellt es für 77 Prozent der Unternehmen eine große Herausforderung dar, integrierte Cloud-Management-Tools im IT-Service-Management einzuführen. Während es am Markt bereits eine ganze Reihe von Cloud-Management-Tools gibt, besteht die Schwierigkeit bei Hybrid- und/oder Multi-Cloud-Szenarien in ihrer Vernetzung zu einem Gesamtsystem und somit in einer integrierten Steuerung eines Geschäftsprozesses über mehrere Deployments und Cloud-Anbieter hinweg.

Als unmittelbare Folge einer höheren Komplexität in der Steuerung von Cloud-Landschaften und steigender Compliance-Anforderungen besteht in fast allen Unternehmen großer Anpassungsbedarf – vor allem im IT-Security-, Configuration- und Capacity-and-Performance-Management, aber auch im Compliance-Bereich.

Mehr Cloud-Nutzung führt zu starkem Optimierungsbedarf im IT Service Management

In welchen der folgenden Prozesse des IT-Service-Managements sehen Sie durch die Nutzung von hybriden/multiplen Cloud-Modellen Anpassungsbedarf?

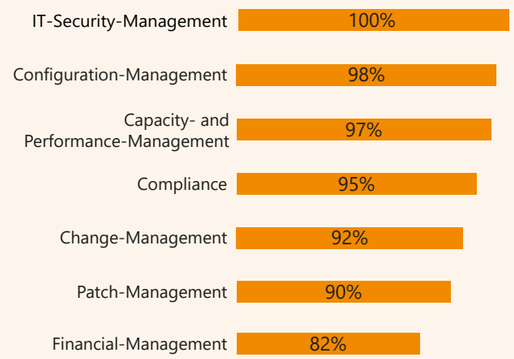


ABB. 5.5: LÜNENDONK®-STUDIE „DER MARKT FÜR IT-SOURCING-BERATUNG IN DEUTSCHLAND“ 2022, SKALA VON 1 =„KEINE OPTIMIERUNG NOTWENDIG“ BIS 5 = „SEHR GROSSE OPTIMIERUNG NOTWENDIG“; ALLE TEILNEHMER; N = 101

Compliance und Sicherheit der Cloud-Transformation – die geteilte Verantwortung im Blick behalten

Von Jörg Botsch und Aleksei Resetko

Auch wenn Cloud-Anbieter compliant sind, müssen Nutzer sich selbst um die Sicherheit und Compliance ihrer Cloud kümmern. Welche Fallstricke sollten sie vermeiden – und welche Best Practices gibt es?

Die Cloud-Transformation ist ein wesentlicher Bestandteil der digitalen Unternehmenstransformation. Unternehmen nutzen vermehrt Cloud-Dienste, um rasch Lösungen zu implementieren, die das Kerngeschäft an die digitalisierte Welt anpassen oder neue Geschäftsmodelle ermöglichen. Agilität, Skalierbarkeit und Kosteneffizienz lassen sich mit Cloud-Services meist deutlich besser erreichen als ausschließlich mit der unternehmenseigenen IT-Infrastruktur.

Dabei ist jedoch zu beachten: Zwar richten die meisten Cloud-Provider ihre Dienste an den relevantesten Compliance-Standards ihrer Kunden aus, doch sind Cloud-Nutzer letztlich selbst dafür verantwortlich, Compliance-Vorschriften einzuhalten und für größtmögliche Sicherheit zu sorgen. Bei der Cloud-Nutzung gilt das Prinzip der geteilten Verantwortung („Shared Responsibility"). Doch warum gewährleisten die Compliance und Sicherheit des Cloud-Providers nicht automatisch die der Nutzer?

Auf die richtigen Nachweise achten

Was genau bedeutet „geteilte Verantwortung" zwischen Cloud-Providern und -Nutzern? Provider stellen eine solide Basisinfrastruktur bereit und kümmern sich vollumfänglich um die physische Sicherheit, um IT-Hardware wie Server, Speicher und Netzwerktechnik und die jeweiligen Virtualisierungsschichten. Dies bezeichnet man auch als „Infrastructure as a Service" (IaaS). In diesem Modell sind die Cloud-Nutzer aber weiterhin dafür verantwortlich, für Anwendungen, Daten und Betriebssysteme angemessene Sicherheitsmaßnahmen zu ergreifen, welche die für das eigene Unternehmen relevanten Compliance- und Sicherheitsanforderungen erfüllen. Bei den weiteren Cloud-Service-Modellen wie „Platform as a Service" (PaaS) oder „Software as a Service" (SaaS) nimmt der Anteil der Verantwortung des Cloud-Nutzers zwar weiter ab, ist aber für Einzelbereiche wie z. B. eine angemessene Nutzerverwaltung immer noch gegeben.

Dass Compliance-Vorgaben auf angemessene Weise erfüllt werden, weisen Cloud-Provider im Wesentlichen mit Zertifizierungen nach. Wichtig sind vor allem solche, die nachweisen, dass angemessene Kontrollen über einen definierten Zeitraum wirksam sind – anstatt die Einrichtung eines Managementsystems stichtagsbezogen zu bestätigen. Zeitraumbezogene Prüfungen weisen für den jeweiligen Zeitraum nach, dass die eingerichteten Kontrollen im Berichtszeitraum mit hinreichender Sicherheit wirksam waren. Zeitraumbezogene Bescheinigungen, auf die Cloud-Nutzer bei Cloud-Providern vor allem achten sollten, sind unter anderem:

- Cloud Computing Compliance Criteria Catalogue vom Bundesamt für Sicherheit in der Informationstechnik (BSI C5) oder
- SOC1- und SOC2-Reports des AICPA (Amerikanisches Institut für Wirtschaftsprüfer) oder
- International Standard on Assurance Engagements zur Prüfung eines internen Kontrollsystems bei einem Dienstleistungsunternehmen (ISAE 3402).

Best Practices für die Cloud-Compliance

Weiterhin gehen Cloud-Nutzer häufig fälschlicherweise davon aus, dass die Compliance-Zertifizierungen des Cloud-Providers automatisch die eigene Compliance bedeutet. Es ist jedoch – wie zuvor ausgeführt – nur ein Teil der Gleichung, wenn führende Cloud-Anbieter wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud viele Sicherheits- und Compliance-Standards erfüllen.

Cloud-Nutzer müssen die eigenen Compliance-Anforderungen identifizieren und sicherstellen, dass ihre und die Maßnahmen des Providers im Zusammenspiel die eigenen Anforderungen insgesamt erfüllen.

Um die Compliance der Cloud-Transformation zu gewährleisten, sollten Nutzer daher diese bewährten Schritte befolgen:

1. **Compliance-Anforderungen verstehen:** Identifizieren Sie die branchenspezifischen und -übergreifenden Compliance-Anforderungen, die Ihr Unternehmen betreffen.
2. **Compliance-Anforderungen in interne Vorgaben übersetzen:** Übersetzen Sie die identifizierten Anforderungen in interne Regelungen (Policies) und Vorgaben. Stellen Sie außerdem sicher, dass diese den betroffenen Bereichen und Personen bekannt sind.
3. **Prozesse anpassen und Kontrollen implementieren:** Implementieren Sie angemessene Sicherheitskontrollen für Ihre Anwendungen und Daten in der Cloud, um Compliance- und Sicherheitsrisiken zu minimieren.
4. **Überprüfung der Compliance des Cloud-Providers:** Überprüfen Sie, ob und inwiefern der Cloud-Provider die notwendigen Compliance-Standards erfüllt und ob entsprechende Zertifizierungen vorliegen.
5. **Vertragliche Vereinbarungen prüfen:** Achten Sie auf die vertraglichen Vereinbarungen mit dem Cloud-Provider und stellen Sie sicher, dass diese Ihre Compliance-Anforderungen abdecken.

ABB. 6.1: BEWÄHRTE PRAKTIKEN UM DIE COMPLIANCE DER CLOUD-NUTZUNG SICHERZUSTELLEN

Die Sicherheit gehört zum Kern der Cloud-Transformationsstrategie

Transformieren Unternehmen ihre Anwendungen in die Cloud, müssen sie neben der Compliance auch Sicherheitsaspekte berücksichtigen. Dies trifft insbesondere auch dann zu, wenn sie dafür Low- bzw. No-Code-Plattformen oder Container-Technologien wie Docker nutzen. Die Erfahrung zeigt hier häufig, dass gerade bei den einfach zu nutzenden Plattformen selbst essenzielle Sicherheitsmaßnahmen nicht umgesetzt werden. Aus sicherheitstechnischer Sicht sollten daher, gerade auch bei der Anwendungstransformation, folgende Punkte unbedingt berücksichtigt werden:

1 **Datensicherheit:** Der Datenschutz hat oberste Priorität bei der Migration von Anwendungen in die Cloud. Sie sollten bewerten, wie sensibel Ihre Daten sind, und sie angemessen schützen – beispielsweise mit Verschlüsselung, Zugriffskontrollen und Mechanismen, die Datenverlust und unbefugten Zugriff verhindern.

2 **Identitäts- und Zugriffsmanagement:** Ein robuster Identitäts- und Zugriffsmanagementansatz (IAM) ist für Cloud-Nutzer unerlässlich. Mit starken Authentifizierungsmechanismen wie Multifaktorauthentifizierung und dem Prinzip der minimalen Rechte stellen Sie sicher, dass nur autorisierte Personen auf Cloud-Ressourcen und -anwendungen zugreifen.

3 **Sicherheitsgerechte Entwicklung:** Im Zuge der Anwendungstransformation ist es entscheidend, sichere Entwicklungspraktiken zu befolgen und Sicherheit in den Softwareentwicklungsprozess zu integrieren. Hierzu gehören regelmäßige Sicherheitstests, Schwachstellenanalysen und Code Reviews, um potenzielle Sicherheitslücken in den Anwendungen zu identifizieren und zu beheben, bevor diese in der Cloud bereitgestellt werden.

4 **Sicherheitsbewusstsein der Entwickler:** Auch wenn Low- bzw. No-Code-Plattformen den Entwicklungsprozess erleichtern, ist es wichtig, dass die Entwickler ein grundlegendes Sicherheitsbewusstsein haben. Sie sollten über gängige Sicherheitslücken und Schwachstellen informiert sein und Best Practices für die Sicherheit von Anwendungen verstehen. Regelmäßige Schulungen und Sensibilisierungskampagnen können dazu beitragen, das Sicherheitsbewusstsein zu stärken.

5 **Orchestrierungssicherheit:** Wenn Sie Container-Orchestrierungstools wie Kubernetes verwenden, sollten Sie sicherstellen, dass diese sicher konfiguriert sind. Implementieren Sie Sicherheitsrichtlinien für die Orchestrierung, verwenden Sie sichere Kommunikationskanäle und stellen Sie sicher, dass die Zugriffskontrolle angemessen verwaltet wird.

6 **Ressourcenbegrenzung:** Legen Sie Ressourcenbegrenzungen für Container fest, um sicherzustellen, dass diese nicht übermäßig viele Ressourcen verbrauchen oder andere Container beeinträchtigen. Dies hilft, Container effizient und sicher auszuführen.

7 **Netzwerksicherheit:** Implementieren Sie, neben den Maßnahmen des Anbieters, eigene angemessene Sicherheitsmaßnahmen auf Netzwerkebene, um Ihre Anwendungen und Daten vor unbefugtem Zugriff und Angriffen zu schützen. Dies erreichen Sie beispielsweise mit virtuellen privaten Netzwerken (VPNs), Webapplikation-Firewalls (WAF) und indem Sie Intrusion Detection and Prevention Systems (IDPS) implementieren, um den Netzwerkverkehr zu überwachen und zu schützen.

8 **Incident Response und Überwachung:** Sehr wichtig ist außerdem, dass Sie einen Incident-Response-Plan und robuste Überwachungsfunktionen implementieren. Sie sollten Ihre Anwendungen und Infrastruktur auch proaktiv auf verdächtige Aktivitäten oder Sicherheitsvorfälle überwachen. Dadurch erkennen Sie Bedrohungen und Sicherheitsverletzungen frühzeitig und können sie abwehren. Verlassen Sie sich an dieser Stelle nicht darauf, dass Ihr Cloud-Provider dies automatisch für Sie übernimmt. Stellen Sie sicher, dass vorhandene Sicherheitslösungen auch tatsächlich genutzt werden.

9 **Software as a Service (SaaS):** Eine besondere Herausforderung ist die Sicherheit von SaaS. Viele SaaS-Anbieter entwickeln proprietäre Sicherheitsmechanismen, die in die vorhandene Sicherheitsarchitektur integriert werden müssen. Zum Beispiel bringt das Identitäts- und Zugriffsmanagement häufig einen Mehraufwand bei der sicheren Integration mit sich.

Sicherer Weg in die Cloud

Festzuhalten bleibt: Die Compliance und Sicherheit des Cloud-Providers gewährleisten nicht automatisch die der Cloud-Nutzer: Es gilt das Prinzip der geteilten Verantwortung. Verstöße gegen Compliance-Vorschriften können schwerwiegende Konsequenzen für Unternehmen haben: Sanktionen, Geldstrafen und Reputationsverlust sind nur einige der möglichen Auswirkungen. Solche mit der Cloud-Nutzung verbundenen Risiken minimieren Sie mit proaktiven Maßnahmen – und nutzen die Vorteile der Cloud-Transformation in vollem Umfang. Dies gelingt allerdings nur, wenn Unternehmen, auch unterstützt durch erfahrene Experten, typische – und untypische – Risiken der Cloud-Transformation in den Blick nehmen.

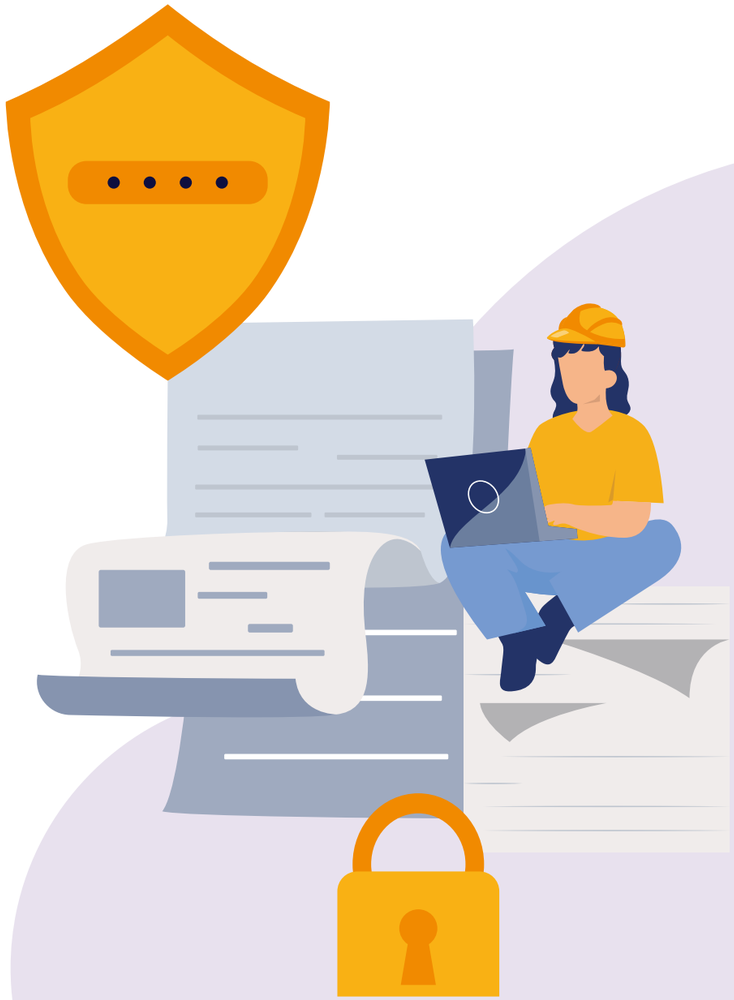
Cloud Security – individuelle Risiken und effektive Maßnahmen

Von Jens Westphal

Die Migration in die Cloud ist für zahlreiche Unternehmen ein entscheidender Schritt auf dem Pfad der digitalen Transformation. Sie birgt viele Vorteile, konfrontiert uns jedoch gleichzeitig mit einer Reihe von Herausforderungen. Um diese erfolgreich zu bewältigen, ist es von grundlegender Bedeutung, sämtliche Risiken und Bedrohungen individuell abzuwägen und geeignete Maßnahmen zu ergreifen.

In einer Welt, die immer stärker auf Technologie setzt und insbesondere die Cloud-Technologie favorisiert, nimmt die Relevanz des Themas Cybersicherheit unaufhörlich zu. Dieser Aspekt und die schwer einzuschätzenden Risiken bewegen einige Unternehmen jedoch immer noch dazu, vor dem großen Sprung in die Cloud zurückzuschrecken. Im Zentrum ihrer Bedenken stehen dabei Datensicherheit, Datenschutz und Compliance-Anforderungen, denn die Dezentralisierung von Daten kann Unsicherheit erzeugen.

Die Cloud bietet bei Sicherheitsaspekten Vorteile, aber auch Herausforderungen. Für bestimmte Bedrohungsarten entstehen Vorteile, dafür kommen neue Bedrohungsarten hinzu. Dabei gilt es, verschiedene Dimensionen und Szenarien zu betrachten. Die spezifischen Herausforderungen bei der Implementierung von Cloud-Diensten variieren in Abhängigkeit von der Art der durch Unternehmen verarbeiteten Daten, der Unternehmensgröße, der Branche und vielen weiteren Faktoren. So gehen stark regulierte Branchen oftmals mit sensiblen und vertraulichen Daten um, die einen besonderen gesetzlichen Schutz haben. Hier führen beispielsweise spezifische Branchenvorgaben zu strikten Compliance-Anforderungen, die in der Cloud-Umgebung neue Herausforderungen nach sich ziehen. Gefragt sind eine durchdachte Sicherheitsstrategie und eine gut geplante Umsetzung.



Unternehmensspezifische Herausforderungen bei der Cloud-Implementierung

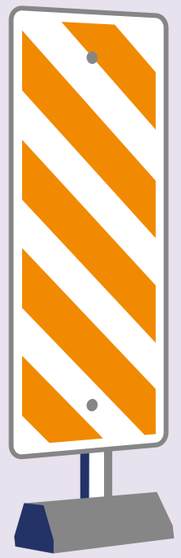
Die Frage „Wie sicher ist die Cloud?“ wird oftmals zu allgemein und zu pauschal beantwortet. Aussagekräftiger ist die Diskussion der Frage: Was kann einem Unternehmen bei einem Angriff tatsächlich passieren? Entscheidend ist, welche Daten und Anwendungen in der Cloud verarbeitet werden und welchen Wert sie für Dritte haben. Ein einfaches Beispiel aus dem täglichen Leben könnte eine Gartenhütte sein, in der lediglich alte Gartengeräte lagern. Hier genügt ein einfaches Schloss zur Absicherung. Anders ist es, wenn in der Hütte Goldbarren aufbewahrt werden. Hier muss man sicherlich stärkere Schutzmaßnahmen ergreifen. Analog dazu müssen in der Cloud gespeicherte Daten und Anwendungen je nach Wichtigkeit und Sensibilität unterschiedlich geschützt werden.

Unbestreitbare Vorteile bietet die Cloud in Bezug auf die Verfügbarkeit und Wiederherstellbarkeit von Systemen. Wenn beispielsweise im klassischen Falle des eigenen Rechenzentrums nach einem erfolgreichen Angriff der gesamte Hardwarebestand als nicht mehr vertrauenswürdig angesehen werden muss, da jedes betroffene System und jeder Server kompromittiert und damit ein potentielles dauerhaftes Risiko darstellen könnte, stünde das Unternehmen vor der gewaltigen Aufgabe, seine IT-Infrastruktur vollständig neu aufzubauen. Das ist sowohl zeitaufwendig als auch kostenintensiv. Lägen alle Systeme in der Cloud, könnte das Unternehmen agiler und effizienter handeln. Das infizierte System in der Cloud ließe sich einfach abschalten und neu aufbauen – eine wesentlich kostengünstigere Lösung im Vergleich zum Neuaufbau einer physischen IT-Infrastruktur. Darüber hinaus kann eine rasche Wiederherstellung des Betriebs nach einem Angriff den Schaden begrenzen und die Ausfallzeit minimieren.

Bedrohungsanalyse als Ausgangspunkt für die Risikobewertung

Cloud-Sicherheit erfordert eine kontinuierliche Risikobewertung und Maßnahmenanpassung, um mit der dynamischen Bedrohungsentwicklung Schritt zu halten. Nur so kann ein Unternehmen die Vorteile der Cloud nutzen, ohne dabei seine Daten und Systeme zu gefährden. Jedes Unternehmen muss zusätzlich zu den Standard-Sicherheitsmaßnahmen der Cloud-Dienste immer eine eigene, auf das individuelle Unternehmen zugeschnittene Risikobewertung durchführen sowie eine eigene Sicherheitsstrategie entwickeln und umsetzen.

Ein Risiko entsteht grundsätzlich immer dann, wenn eine Bedrohung auf eine Schwachstelle trifft. Da sich die Bedrohungen stetig verändern und ständig neue Schwachstellen aufgedeckt werden, ist ein kontinuierlicher Prozess zur Risikominimierung erforderlich. Zur Bewertung der Bedrohungslage muss daher jeder Bedrohungsvektor einzeln anhand der Anforderungen und der Situation des jeweiligen Unternehmens und seiner IT-Infrastruktur bewertet werden. Während traditionell in der IT-Sicherheit die Hauptbedrohungen im Bereich der physischen und netzwerkbasierten Sicherheit liegen, verändert die Migration in die Cloud diese Bedrohungsvektoren. Die physische Absicherung von Serverräumen liegt nun hauptsächlich beim Cloud-Anbieter. In den Fokus der Risikobewertung rücken stattdessen Bereiche wie Zugriffskontrolle und Identitätsmanagement, Datenverschlüsselung, sicheres Design und die Konfiguration von Cloud-Diensten.



Der Weg zu einer ausgewogenen Risikobewertung

Der Prozess zur Erstellung einer ausgewogenen Risikobewertung für die Nutzung von Cloud-Umgebungen erfordert ein systematisches Vorgehen. Ziel ist es, ein Gleichgewicht zwischen den geschäftlichen Vorteilen der Cloud und potenziellen Sicherheitsrisiken zu finden. Dies erfordert die Zusammenarbeit verschiedener Spezialisten, etwa eines Cloud-Architekten und eines Sicherheitsspezialisten. In der Praxis beginnt der Prozess mit einer Bestandsaufnahme der bestehenden IT-Systeme und einer Einschätzung, welche davon in die Cloud migriert werden sollten. Daraufhin modelliert der Cloud-Architekt, der einen umfassenden Überblick über die gesamte IT-Landschaft besitzt, eine Zielarchitektur. Parallel dazu wird ein Cloud-Security-Spezialist hinzugezogen, der die potenziellen Bedrohungsvektoren in der geplanten Architektur und während des Transformationsprozesses identifiziert und daraus entsprechende Sicherheitsmaßnahmen ableitet.

Dieser Prozess erinnert an den Bau eines Hauses, bei dem Architekten und Statiker zusammenarbeiten. Der Cloud-Security-Spezialist hat eine ähnliche Funktion wie ein Statiker beim Hausbau. Er muss verstehen, wie bestimmte Elemente miteinander interagieren und wo Anpassungen erforderlich sind. Seine Expertise und Kenntnisse, zum Beispiel in Bezug auf Methoden und Standards wie C5 oder Mobile Office Records, sind entscheidend, um die Sicherheitsstruktur zu optimieren. So wie ein erfahrener Statiker baufällige Strukturen identifizieren und verbessern kann, bevor das Risiko eines Einsturzes entsteht, hat ein Cloud-Security-Spezialist Erfahrung mit problematischen Sicherheitsszenarien. Mit den vom Sicherheitsspezialisten erarbeiteten Informationen kann der Cloud-Architekt dann entscheiden, wie beispielsweise das „Prinzip Zero Trust“ oder andere Sicherheitsmechanismen umgesetzt werden. Das ausgearbeitete Sicherheitskonzept wird schriftlich festgehalten, detailliert beschrieben und kann als Referenz und für Prüfungen und Audits herangezogen werden.

Umsetzung der Migration in die Cloud

Anschließend wird die Cloud-Umgebung aufgebaut und eine Prüfung durchgeführt, um sicherzustellen, dass alles wie im Sicherheitskonzept beschrieben umgesetzt wurde. Ähnlich wie bei einem Hausbau kann ein externer Prüfer das Konzept bestätigen und eine Art „Baugenehmigung“ erteilen. Nach Abschluss der Prüfung und Bereitstellung der Cloud-Umgebung wird die Migration durchgeführt. Dabei ist die Reihenfolge, in der die Dienste eingeführt werden, entscheidend. Spezialisierte Dienstleistungen, wie das „Security Incident Event Management“ (SIEM), spielen in diesem Kontext eine wichtige Rolle. SIEM-Systeme bieten Echtzeit-Analysen von sicherheitsrelevanten Vorkommnissen und Log-Daten, die von Netzwerkhardware und -anwendungen generiert werden. Sie helfen dabei, irregulären Betrieb zu erkennen und rechtzeitig zu reagieren. Allerdings erfordert die Überwachung dieser Systeme qualifizierte Expertise. Unternehmen benötigen daher entweder interne Spezialisten oder externe Dienstleistungen, um die Funktionsfähigkeit der Sicherheitssysteme ständig gewährleisten zu können.

Die Bedeutung von Sicherheit nach der Migration

Weitere fortlaufende Dienstleistungen umfassen regelmäßige technische Analysen, Penetrationstests, Organisationsanalysen und Audits, um sicherzustellen, dass das implementierte System dauerhaft funktioniert und an die sich ständig ändernde Bedrohungslage angepasst wird. Dabei ist es wichtig, dass die Dienstleistungen zu den Geschäftszielen und Bedürfnissen des Unternehmens passen. Ein effektiver Schutz muss dabei auch wirtschaftlich sein. Daher sollte die Dimensionierung der Sicherheitsziele immer so erfolgen, dass sie erreicht werden können, ohne die finanzielle Stabilität des Unternehmens zu gefährden.

Ein entscheidender Faktor in diesem Prozess ist das Vertrauen. Die Unternehmen müssen darauf vertrauen können, dass IT-Sicherheitsdienstleister die Interessen des Unternehmens im Blick haben und dass sie die geschäftlichen Aspekte ebenso verstehen wie die technischen. Dieser Vertrauensaufbau durch ein tiefes Verständnis des Geschäfts und die Bereitstellung effektiver, wirtschaftlich sinnvoller Lösungen kann letztlich den Grundstein für langjährige, produktive Zusammenarbeit legen.

Cybersicherheit: Bleiben Sie dran!

In der sich stetig wandelnden digitalen Landschaft sind eine robuste Cloud-Sicherheitsstrategie, eine sorgfältige Umsetzung und regelmäßige Überprüfungen nicht mehr nur wünschenswert, sondern unumgänglich. Gleichzeitig benötigen wir einen kulturellen Wandel, der die Bedeutung von Datensicherheit in der Cloud verankert.

Während wir uns in eine neue Ära der Cloud-Sicherheit bewegen, geprägt durch technologische Innovationen und ein gesteigertes Nutzerbewusstsein, erinnert uns der ständige Fortschritt daran, dass wir kontinuierlich anpassungsfähig und lernbereit sein müssen. Denn Cloud-Sicherheit ist kein statisches Ziel, sondern eine dynamische Herausforderung, bei der wir stets bestrebt sein müssen, einen Schritt voraus zu sein, damit die Cloud ein sicherer und vertrauenswürdiger Ort für all unsere digitalen Bedürfnisse ist und bleibt.

Autorenprofile

Dr. Manuel Audi
msg advisors

Dr. Manuel Audi ist Geschäftsführer der BELTIOS GmbH, dem zur msg-Gruppe gehörenden Beratungsunternehmen für die Versicherungswirtschaft. Als Teil der msg advisors leitet er den Bereich Business Consulting Insurance und begleitet Versicherungsunternehmen insbesondere bei den Themen digitale Transformation, Vertriebsoptimierung, Prozessoptimierung und Restrukturierung. Dr. Audi bringt über 16 Jahre Erfahrung bei der Beratung von Versicherungsunternehmen mit und hat viele Versicherer erfolgreich bei der Neuausrichtung ihrer Geschäfts- und Betriebsmodelle unterstützt, so auch bei Internationalisierungsstrategien und der Cloud-Transformation.

Kontakt:
Dr. Manuel Audi
Geschäftsführer des msg-Beratungsunternehmens BELTIOS

E-Mail: manuel.audi@beltios.com
LinkedIn: https://www.linkedin.com/in/manuelaudi/

▶ **Artikel „International wachsen durch Cloud-Technologie – darauf sollten Unternehmen achten", S. 38**

Jörg Botsch
PwC

Jörg Botsch ist Partner bei PwC Deutschland, Leiter der IT Reliability & Compliance Practice und Teil des Cloud Transformation Center of Excellence. Als Diplom-Wirtschaftsingenieur des KIT hat er fast 20 Jahre Erfahrung im IT-Bereich und ist gefragter Ansprechpartner für alle Fragen rund um den zuverlässigen, resilienten und regelkonformen IT-Betrieb unter Einsatz von Cloud-Diensten, auch in hybriden Szenarien mit eigener IT-Infrastruktur.

Kontakt:
Jörg Botsch
Partner, PwC

E-Mail: joerg.botsch@pwc.com
LinkedIn: https://www.linkedin.com/in/joerg-botsch/

▶ **Artikel „Compliance und Sicherheit der Cloud-Transformation – die geteilte Verantwortung im Blick behalten", S. 50**

Friederike Frommann
PwC

Friederike Frommann ist Senior Managerin im Bereich Cloud & Digital bei PwC am Standort Frankfurt. Seit zehn Jahren leitet sie branchenübergreifend große digitale Transformationen im Bereich Cloud und Modern Work. Ihr Schwerpunkt liegt in den Bereichen IT-Strategie, App-Modernisierung und digitale Innovation.

Kontakt:
Friederike Frommann
Senior Managerin, PwC

E-Mail: friederike.frommann@pwc.com
LinkedIn: https://www.linkedin.com/in/friederike-frommann-3431304b/

▶ **Artikel „Die Zukunft der Anwendungsmodernisierung und Cloud-Transformation", S. 12**

Autorenprofile

Thilo Mundt
COSMO CONSULT

Thilo Mundt blickt auf eine langjährige internationale Erfahrung im ERP- und Projektmanagement zurück. Als Initiator und Verantwortlicher der Business-Unit „Customer Strategy Management" arbeitet der diplomierte Wirtschaftswissenschaftler in einer Schlüsselposition von COSMO CONSULT. Hier entwickelt er unter anderem neue Konzepte für ein Customer Centric Consulting, das die technologischen, strategischen und kulturellen Aspekte der digitalen Transformation zusammenführt.

Kontakt:
Thilo Mundt
Lead Customer Strategy Management, COSMO CONSULT

E-Mail: thilo.mundt@cosmoconsult.com
LinkedIn: https://www.linkedin.com/in/thilo-mundt-3b6129a1/

▶ **Artikel „Warum es an der Zeit ist, Consulting neu zu denken", S. 24**

Sebastian Paas
PwC

Sebastian Paas ist Partner und Leader für den Bereich Cloud & Digital bei PwC. Er verfügt über mehr als 20 Jahre Berufserfahrung in der Technologieberatung und ist spezialisiert auf die Planung und das Management großer IT-Transformationen sowie IT-Strategiefragen. Er ist regelmäßiger Blogger und Gastdozent an der renommierten ESCP Europe.

Kontakt:
Sebastian Paas
Partner, PwC

E-Mail: sebastian.paas@pwc.com
LinkedIn: https://www.linkedin.com/in/sebastian-paas-%E2%98%81-b2683257/

▶ **Artikel „Die Zukunft der Anwendungsmodernisierung und Cloud-Transformation", S. 12**

Aleksei Resetko
PwC

Aleksei Resetko ist Partner bei PwC Cybersecurity & Privacy und leitet die EMEA Cloud Security Praxis. Er hat Wirtschaftswissenschaften an der Universität Heidelberg studiert und kann auf mehr als 20 Jahre Berufserfahrung zurückgreifen. Darüber hinaus besitzt Aleksei Resetko die Zertifizierungen CISA und CISSP. Mit verschiedenen fachspezifischen Referententätigkeiten und wissenschaftlichen Veröffentlichungen zu den Themen Cloud-Compliance und -Sicherheit hat er seine Expertise vielfach bewiesen.

Kontakt:
Aleksei Resetko
Partner, PwC

E-Mail: aleksei.resetko@pwc.com
LinkedIn: https://www.linkedin.com/in/alekseiresetko/

▶ **Artikel „Compliance und Sicherheit der Cloud-Transformation – die geteilte Verantwortung im Blick behalten", S. 50**

Autorenprofile

Dr. Stefan Schnitter
Detecon

Dr. Stefan Schnitter ist Managing Partner und Experte für Cloud-Transformation. Zuvor war er als Managing Director und Vice President Infrastructure bei der Deutschen Telekom PanNet für die europaweite Bereitstellung von Cloud-Infrastruktur und Cloud-basierten Telekommunikationsdiensten zuständig. Er betrachtet Cloud-bezogene Beratungsthemen aus einem breiten Blickwinkel, d.h. aus Strategie-, Infrastruktur-, Anwendungs-, Technologie-, Organisations-, Prozess- oder Kulturperspektive. Zielgruppe seiner branchenübergreifenden Aktivitäten sind Kunden aus den Branchen Telekommunikation, Automobil, Fertigung und Dienstleistung.

Kontakt:
Dr. Stefan Schnitter
Managing Partner, Detecon

E-Mail: stefan.schnitter@detecon.com
LinkedIn: https://www.linkedin.com/in/stefan-schnitter-8b046922/

▶ Artikel „FinOps – ein Vorgehensmodell für optimierte Cloud-Kosten“, S. 20
▶ Artikel „Edge Computing ist ein Enabler für Echtzeit, Datenschutz und Nachhaltigkeit“, S. 28

Jens Westphal
msg advisors

Jens Westphal leitet das Geschäftsfeld msg security advisors, das das Beratungs-Know-how der msg-Gruppe im IT-Security-Umfeld bündelt. Der IT-Sicherheitsexperte bringt über 25 Jahre Erfahrung in der Security-Branche mit und ist unter anderem in den Feldern Public Sector und kritische Infrastrukturen tätig. Er ist ausgewiesener Spezialist für den Aufbau und Betrieb von Informationssicherheitsmanagementsystemen nach ISO 27001 sowie für den IT-Grundschutz und unterstützt Organisationen branchenübergreifend dabei, Cyber-Resilienz im Kern der Geschäftstätigkeiten zu verankern, um so die Grundlage für eine erfolgreiche Transformation zu schaffen.

Kontakt:
Jens Westphal
Geschäftsleitung, msg security advisors

E-Mail: jens.westphal@msg.group
LinkedIn: https://www.linkedin.com/in/jens-westphal-7852776a/

▶ Artikel „Cloud Security – individuelle Risiken und effektive Maßnahmen“, S. 54

Mario Zillmann
Lünendonk & Hossenfelder

Mario Zillmann ist gelernter Versicherungskaufmann und war bis 2002 im Key-Account-Management einer öffentlichen Versicherungsanstalt tätig. Bis 2006 studierte er Betriebswirtschaftslehre an der Fachhochschule für Wirtschaft in Berlin mit den Schwerpunkten Marketing sowie Information und Kommunikation. Seit 2007 ist er bei Lünendonk tätig und verantwortet als Partner Marktforschungs- und Beratungsprojekte in den Märkten IT-Dienstleistungen, Engineering Services und Digital Experience Services.

Kontakt:
Mario Zillmann
Partner, Lünendonk & Hossenfelder

E-Mail: zillmann@luenendonk.de
LinkedIn: https://www.linkedin.com/in/mario-zillmann-21878111/

▶ Artikel „Cloud-Transformation – Element der digitalen Transformation“, S. 6
▶ Artikel „Herausforderungen der Cloud-Transformation“, S. 46

Autorenprofile/Interviewprofile

Christian Krause
COSMO CONSULT

Christian Krause, der seit inzwischen fast 30 Jahren im IT-Sektor arbeitet, ist die treibende Kraft hinter der COSMO-Cloud. Bereits während seines Studiums der Betriebswirtschaft beschäftigte er sich intensiv mit Infrastruktur-Technologien. Nach dem Diplom war er in leitenden Positionen für namhafte ERP- und ECM-Anbieter tätig, bevor er 2016 die Verantwortung für die Konzeption und den Betrieb der Microsoft-Azure-basierten Managed-Services-Plattform von COSMO CONSULT übernahm.

Kontakt:
Christian Krause
Lead Operations Management, COSMO CONSULT

E-Mail: christian.krause@cosmoconsult.com
LinkedIn: https://www.linkedin.com/in/christian-krause-ardent4cloud/

▶ Artikel „Eat your own dog food“, S. 16

Marcus Neumann
Materna

Marcus Neumann ist Vice President Cloud Innovation & Operation bei Materna im Ressort Industries. Für das Fokusfeld Journey2Cloud™ ist er übergreifend bei Materna verantwortlich. Seit mehr als 25 Jahren ist er in der IT-Branche in verschiedenen Management-Positionen tätig – sowohl in der Industrie als auch im Bereich Public Sector. Seit fast zwei Jahrzehnten begleitet Marcus Neumann angehende IT-Profis als Prüfer für den Ausbildungsberuf Fachinformatiker Systemintegration bei der Handelskammer Hamburg.

Kontakt:
Marcus Neumann
Vice President Cloud Innovation & Operation, Materna

E-Mail: marcus.neumann@materna.group
LinkedIn: https://www.linkedin.com/in/marcusneumann/

▶ Artikel „Erfolgreiche Cloud-Migration: Die Applikation steht im Mittelpunkt“, S. 32
▶ Artikel „Governance ist der Schlüssel zu sicheren und nachhaltigen Cloud-Lösungen“, S. 42

Benjamin Springub
Telekom Deutschland

Benjamin Springub ist Vice President Operations Development bei der Telekom Deutschland GmbH. Zusätzlich leitet er bei der Telekom das Konzernprogramm „Schubkraft“. Er verantwortet unter anderem Themen wie interne Digitalisierung, Steuerung der operativen Delivery-Bereiche sowie Build and Run Management. Vor seiner aktuellen Position bekleidete er verschiedene Führungsrollen bei der Telekom Deutschland und der T-Systems, wo er für die interne Kommunikation, das Beteiligungsmanagement, die Geschäftsentwicklung und die strategische Ausrichtung zuständig war. Zusätzlich zu seiner beruflichen Laufbahn hat er internationale Erfahrungen gesammelt, unter anderem in Singapur und den USA.

Kontakt:
Benjamin Springub
Vice President Operations Development, Telekom Deutschland

E-Mail: b.springub@telekom.de
LinkedIn: https://www.linkedin.com/in/benjaminspringub/

▶ Artikel „Edge Computing ist ein Enabler für Echtzeit, Datenschutz und Nachhaltigkeit“, S. 28

Unternehmensprofile

COSMOCONSULT

Über Cosmo Consult

Mit mehr als 1.400 Mitarbeiterinnen und Mitarbeitern an 49 internationalen Standorten – davon 16 in Deutschland – gehört die COSMO CONSULT-Gruppe zu den weltweit führenden Digitalisierungspartnern in Industrie, Handel und Dienstleistung.

COSMO CONSULT bietet zukunftssichere Branchen- und End-to-End-Businesslösungen sowie ein umfangreiches Beratungsportfolio, um Unternehmen bei der lückenlosen Abbildung ihrer Geschäftsprozesse zu unterstützen. Neben den bewährten Microsoft-ERP- und CRM-Systemen kommen dabei auch modernste digitale Technologien aus den Bereichen Data & Analytics, künstliche Intelligenz, Collaboration, Industrie 4.0 und Human-Capital-Management zum Einsatz.

Im Mittelpunkt: die Menschen

Menschliche Kreativität, Engagement und Leidenschaft sind die Faktoren, die innovative Produkte und Geschäftsfelder erst möglich machen. COSMO CONSULT stellt die Menschen in den Mittelpunkt der digitalen Transformation und entwickelt Systeme, die

- verständlich sind
- sich einfach bedienen lassen
- Wissen transparent machen
- den Menschen im Arbeitsalltag hilfreich zur Seite stehen

Flankiert werden die Lösungen von einem fortschrittlichen Trainings- und Change-Management-Portfolio, das den Menschen in den Unternehmen dabei hilft, sich zu öffnen und die eigene Kreativität für die gemeinsame Sache einzusetzen.

Auf Augenhöhe mit den Kunden

Zu den Kunden von COSMO CONSULT zählen Unternehmen aller Branchen und Größen – vom Start-up über den klassischen Mittelständler bis zum weltumspannenden Konzern. Sie alle haben eine Gemeinsamkeit: Sie sind einzigartig. Jedes Unternehmen verdient es, die besten Lösungen und Services zu bekommen, die es gibt. Zu den Prinzipien von COSMO CONSULT gehört es daher, allen Kunden mit einem tiefen Verständnis für die Unternehmenskultur, die individuellen Prozesse und die Marktanforderungen, mit denen sie täglich konfrontiert sind, zu begegnen.

Mehr Informationen unter:
https://de.cosmoconsult.com

DETECON
CONSULTING

Über Detecon

Detecon ist eine führende, weltweit agierende Management- und Technologieberatung mit Hauptsitz in Deutschland, die seit über 40 Jahren klassisches Management-Consulting mit hoher Technologiekompetenz vereint. Ihr Leistungsschwerpunkt liegt im Bereich der Digitalisierung: Unternehmenskunden erhalten eine ganzheitliche Beratung zu Strategie, Transformation, Digital Innovation und Business Technology. Schwerpunkte liegen in der Telekommunikation sowie in den Fokusbranchen Automotive & Manufacturing, Public, Transport & Logistics und Healthcare.

Das Know-how der Detecon bündelt das Wissen aus erfolgreich abgeschlossenen Beratungsprojekten in über 160 Ländern. Detecon ist ein Tochterunternehmen der T-Systems International, dem herstellerübergreifenden Digitaldienstleister der Deutschen Telekom.

Detecon entwickelt klassische Beratungsmethoden deutlich weiter und passt sie an heutige und künftige Digitalisierungsanforderungen an. Dazu gehört etwa, dass Top-Beratung das Spektrum von Innovation zur Implementierung abdeckt. Zukunftsweisende Digitalberatung erfordert mehr und mehr Technologie-Expertise und ein hohes Maß an Agilität, das die flexible, aber passgenaue Vernetzung von Experten gerade für komplexe, digitale Ökosysteme mit einschließt. Gleichzeitig wird es in der digitalen Beratung immer wichtiger, die Kunden von der Innovation über Prototyping bis hin zur Implementierung zu begleiten.

Daher gründete Detecon bereits 2017 in Berlin das Digital Engineering Center für Cyber Security, Analytical Intelligence, Co-Innovation und Industrial IoT. 2023 eröffnete Detecon als eine der ersten Unternehmensberatungen ein 5G-Campus-Netz in eigenen Open Spaces. Das „FiveGDock“ in der Kölner Bayenwerft dient als Testgelände für konnektivitätsgetriebene Geschäftsprozesse und bietet Orientierung innerhalb vielfältiger Optionen. Der Campus ist in der Lage, unterschiedlichste Use Cases abzubilden, und ermöglicht es Verantwortlichen, entsprechende Schlüsse in Bezug auf die entwickelte Strategie zu ziehen.

Mehr Informationen unter:
https:// www.detecon.com

Unternehmensprofile

Über Materna-Gruppe

Die Materna-Gruppe realisiert seit mehr als 40 Jahren sehr erfolgreich IT- und Digitalisierungsprojekte für Kunden aus Wirtschaft und Verwaltung und beschäftigt weltweit mehr als 3.700 Mitarbeitende. Im Geschäftsjahr 2022 erzielte Materna einen Gruppenumsatz von 554 Millionen Euro. Materna deckt das gesamte Leistungsspektrum eines Full-Service-Dienstleisters für IT- und Digitalisierungsprojekte ab: von der Beratung über die Implementierung bis zum Betrieb. Zum Konzern gehören verschiedene Tochterunternehmen. Materna besitzt Standorte in Europa, Asien und Nordamerika.

Materna begleitet Kunden von der ersten Idee über die Konzeption und Umsetzung bis zum Betrieb und ist mit seinen Lösungen in Wirtschaft und öffentlicher Verwaltung gleichermaßen vertreten. Die Materna-Experten fungieren als Ideengeber, als Ratgeber in Angebotsphasen, bei der Technologiebewertung und der Plattformauswahl, als Implementierungspartner sowie in allen angrenzenden Phasen eines IT-Projekts. Unser Erfolg gründet auf langjährigen und dauerhaften Kundenbeziehungen.

Der Vorstand wird besetzt durch Martin Wibbe (CEO), Dr. René Rüdinger (CFO), Michael Hagedorn (Public Sector & Security) und Uwe Scariot (Enterprise Service Management & Internationalisierung). Gegründet wurde Materna im Jahr 1980 von Dr. Winfried Materna und Helmut an de Meulen, die heute im Aufsichtsrat tätig sind.

Die Materna-Gruppe bündelt Know-how und Kompetenzen entlang von neun Fokusfeldern, mit denen wir maßgeblich die IT-Zukunft mitgestalten möchten. Die Fokusfelder sind: Verwaltung digital, Enterprise Service Management, Passenger Journey, SAP-Transformation, Journey2Cloud™, Cybersecurity, Digital Experience, Nachhaltigkeit & Widerstandsfähigkeit sowie Data Economy. Materna begleitet Kunden über alle diese Fokusfelder hinweg Ende-zu-Ende als Ideengeber, Berater und Umsetzer und verbindet die Markttrends und Technologien miteinander zu mehrwertschaffenden Lösungen – sei es bei marktführenden Themen, Hype-Themen oder Emerging Themen. Abgerundet werden die Fokusfelder von einem innovativen Ökosystem, strategischen Allianzen mit führenden Technologielieferanten sowie umfangreichem Know-how in Transformationsprojekten, Entwicklungskompetenzen und Software-Assets.

Mehr Informationen unter:
https://www.materna.de

Über msg advisors

Die msg advisors gehören zur msg-Gruppe, die mit mehr als 10.000 Mitarbeitenden in 32 Ländern in den Branchen Automotive, Banking, Consumer Products, Food, Healthcare, Insurance, Life Science & Chemicals, Manufacturing, Public Sector, Telecommunications, Travel & Logistics sowie Utilities tätig ist.

Als Beratungsnetzwerk der msg-Gruppe begleiten die msg advisors Transformationsprozesse und unterstützen Unternehmen bei der Konzeption und dem Aufbau branchenübergreifender Ökosysteme. Unser Leistungsportfolio reicht von der Entwicklung branchenspezifischer Zukunftsszenarien über die Transformation und Weiterentwicklung von Geschäftsmodellen bis hin zur organisatorischen, prozessualen und systemischen Umsetzung mit unseren Klienten.

Insbesondere an Schnittstellen, an denen sich Industrien zu neuen Segmenten und Ökosystemen zusammenfügen, entwickeln wir innovative Lösungskonzepte. Dabei kombinieren wir das Know-how der gesamten msg-Gruppe: Das tiefe Branchenverständnis aus über 1.000 funktionsübergreifenden Projekten wird vereint mit fachlicher Expertise sowie absoluter Exzellenz im Umgang mit Technologien und Daten.

Unser Cloud-Leistungsportfolio ist auf das Gelingen der digitalen Transformation ausgerichtet. Wir entwickeln maßgeschneiderte Cloud-Strategien, planen und führen erfolgreiche Cloud-Migrationen durch, optimieren die Cloud-Infrastruktur und -Anwendungslandschaft, um neue digitale Geschäftsmodelle, Ökosysteme und Prozesse zu ermöglichen sowie Leistung, Sicherheit und Kosteneinsparungen zu maximieren. Unser Ziel ist es, Unternehmen bei der Realisierung des vollen Potenzials der Cloud zu unterstützen und nachhaltigen Erfolg zu ermöglichen.

Mehr Informationen unter:
https://advisors.msg.group/

Unternehmensprofile

Über PwC Deutschland

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Netzwerks aus Expertinnen und Experten in 152 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Mehr als 13.000 engagierte Menschen an 21 Standorten. Knapp 2,61 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

Mehr Informationen unter:
https://www.pwc.com

Impressum

Über Lünendonk

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern)analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Digital & IT, Managementberatung, Wirtschaftsprüfung sowie Steuer- und Rechtsberatung, Real Estate Services und Personaldienstleistung (Zeitarbeit, IT-Workforce).

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien“ heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalistinnen und Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Persönlichkeiten mit den Lünendonk B2B Service-Awards aus.

Mehr Informationen unter:
https://www.luenendonk.de

Lünendonk Magazin
Cloud-Strategie, Best Practices, Cloud Security

Herausgeber und Kontakt
Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim
Telefon: +49 8261 7 31 40-0
Telefax: +49 8261 7 31 40-66
E-Mail: info@luenendonk.de
Internet: www.luenendonk.de

Redaktionsleitung
Mario Zillmann
Projektleitung
Daniel Roßwag
Fotos/Illustrationen
Envato Elements: Titel, S.2, 5, 6, 7, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 29, 30, 33, 34, 35, 36, 37, 38, 39, 41, 43, 45, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 68
Konzeption und Gestaltung
K16 GmbH, Hamburg
www.k16.de

Copyright
© Lünendonk & Hossenfelder GmbH 2023
Alle Rechte vorbehalten. Vervielfältigung dieser Unterlage sowie Verwertung ihres Inhalts unzulässig, soweit nicht ausdrücklich zugestanden! Technische Änderungen vorbehalten.
www.luenendonk.de