CORE®

INFORMATIONS-SICHERHEIT UND DATENSCHUTZ AUS DER CLOUD

Compliance durch Automatisierung in sicheren Infrastrukturen

Autoren
Nicolas Freitag
Markus Frik
Dr. Waldemar Grudzien
Nadine Hofmann

Autorenteam
Christian Böhning
Philipp Gampe
Calvin Klee
Ronny Raschkowan

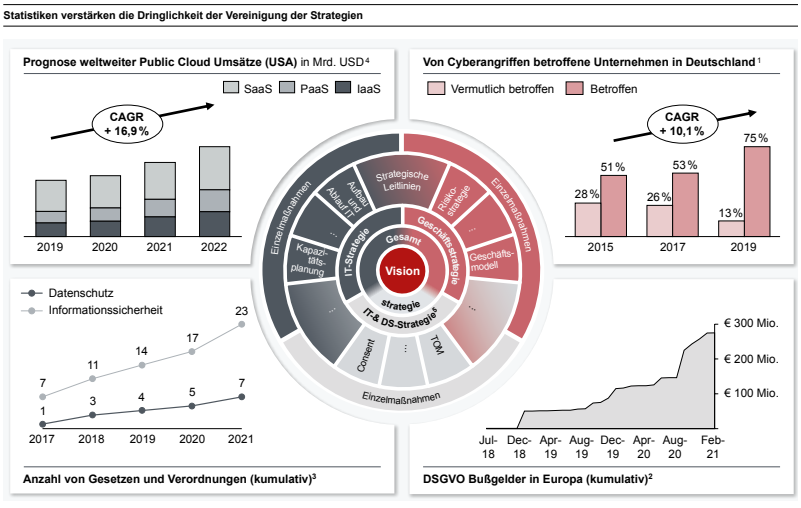
April 2021
White Paper

1 Einleitung

Eigene Hardware ist keine Entschuldigung mehr für einen Verzicht auf die Vorteile der Cloud

Es ist nicht die Frage, ob eine Cloud genutzt wird, sondern wann. Schließlich übt sich eine Organisation mit dem Verzicht auf Cloud-Technologie auch im Verzicht auf immense Vorteile der Cloud und damit auf die eigene Wettbewerbsfähigkeit. Diese Vorteile manifestieren sich in den fünf Aspekten Skalierbarkeit, Innovationspotenzial, Servicequalität, industrielle Softwareentwicklung und Kosteneinsparung. Dabei kann vorweggenommen werden, dass Kosteneinsparung allein die Migration in die Cloud nicht rechtfertigt. Hat eine Organisation ihre IT- und Anwendungslandschaft vollständig im Griff, wird sie allein aus Gründen der Kostensenkung keine Vorteile mehr durch die Migration in die Cloud generieren können. Andernfalls kann die Kostensenkung ein Motivator für eine Migration sein. Der Siegeszug der Cloud lässt sich profan an der jährlich um 17% steigenden weltweiten Umsatzentwicklung ablesen (Teilgrafik links oben in Abbildung 1).

Parallel zum Anwachsen der Möglichkeiten von Hyperscalern (große Anbieter von praktisch unendlich skalierbarer Infrastruktur aus der Cloud), die jenseits der drei üblichen Liefermodelle Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) ganze Öko-Systeme an Tools zur Verfügung stellen, nehmen auch die regulatorischen Anforderungen in Bezug auf Datensicherheit und Datenschutz der Informationsverarbeitung zu. Die Regulierung äußert sich in Gesetzgebung und Aufsichtspraxis in einer vertikalen Verdichtung im Datenschutz und einer horizontalen Ausweitung in der Informationssicherheit. Datenschutz ist ohne entsprechend aufgestellte Datensicherheit nicht möglich. Das zeigt sich allgemein bei einem Cyberangriff, der die Informationssicherheit betrifft und sich oft gleichzeitig als Datenschutzvorfall – mit entsprechenden Bußgeldern – entpuppt.



Quellen: 1 Bitkom Research | 2 CMS | 3 COREresearch | 4 Gartner | 5 Informationssicherheits- & Datenschutzstrategie

Abbildung 1: Informationssicherheit und Datenschutz gewinnen an Relevanz und sollten der Geschäfts- und IT-Strategie ebenbürtig gestaltet werden

Entsprechend sollten beide Sphären als zwei Seiten einer Medaille gesehen und im Rahmen einer einzigen Informationssicherheits- und Datenschutzstrategie behandelt werden. Doch der strategische Ansatz muss geweitet werden: Die Vielfalt der zu berücksichtigenden Compliance-Anforderungen aus Datenschutz und Informationssicherheit stellt alle Marktteilnehmer vor die Herausforderung, die Anforderungen im Rahmen der Digitalisierungs-, IT- und Geschäftsstrategie zu berücksichtigen. Oft werden diese Strategien noch getrennt betrachtet und umgesetzt, sodass das Gesamtbild verengt in separierten Insellösungen umgesetzt wird. Dabei wird eine umfassende Implementierung im Rahmen einer Cloud-Strategie ignoriert.

Exzellenz in eigener Kernkompetenz durch Nutzung der Exzellenz der Cloud

Doch die Cloud ersetzt nicht nur das eigene Rechenzentrum und viele On-Premise Anwendungen zur Bewirtschaftung der eigenen Daten, sie hilft auch bei der Erfüllung von Compliance-Anforderungen: Das automatisierbare Infrastructure-as-Code kann zunehmend mit einem noch manuell zu konfigurierendem Compliance-as-Code (CaC) ergänzt werden. Hyperscaler stellen immer mehr Compliance-Werkzeuge zur Verfügung, welche Anwender in die Lage versetzen, diese Pflichten effizienter und effektiver umzusetzen als bei Eigenbetrieb von Hardware und Anwendungen. Bedingt der Verzicht auf Cloud-Services den Verzicht auf Exzellenz in der eigenen Kernkompetenz, so verstärkt in Umkehrung die Nutzung von Cloud-Services die eigene Exzellenz in der wettbewerbsdifferenzierenden Kernkompetenz. Die in Qualität und Quantität nahezu unendlichen Möglichkeiten einer Cloud sind nur den berühmten einen Klick entfernt.

Das vorliegende Whitepaper zeigt den Weg zu diesem Klick und die damit zu gewinnenden Wettbewerbsvorteile durch Komplexitätsreduktion in kaufmännischer, technisch-organisatorischer und rechtlicher Hinsicht.

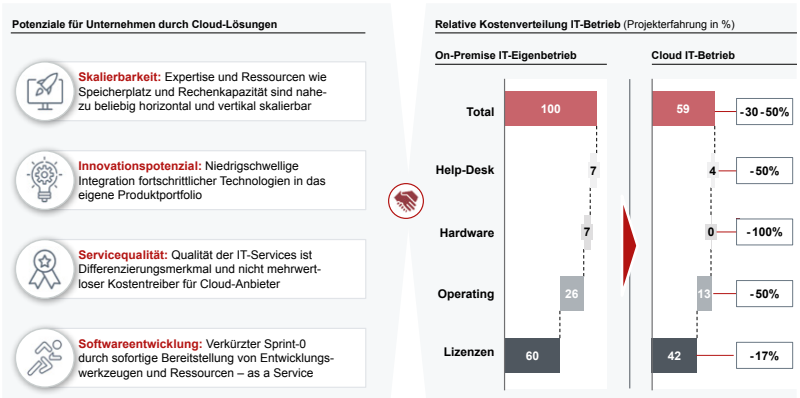
2 Compliance konforme Nutzung der Cloud

Cloud ist keine Frage der Zeit, sondern der Wettbewerbsfähigkeit

Cloud ist nicht mehr in aller Munde, Cloud ist Realität. Hyperscaler bieten in Qualität (Stabilität und Verfügbarkeit eines Angebotes im Sinne von Resilienz) und Quantität (im Sinne von Tools eines Cloud-Ökosystems) Angebote, die immer öfter einen eigenverantwortlichen On-Premise-Betrieb auf den Prüfstand stellen und obsolet machen. Drehte sich in der Anfangszeit der Cloud Mitte der Nullerjahre alles um das Liefermodell, d.h. Eigenbetrieb versus IaaS, PaaS und SaaS, so bieten aktuelle Public Cloud Angebote in ihren Ökosystemen Tools und damit Möglichkeiten der Verarbeitung von Daten, die ein einzelnes Unternehmen qualitativ und quantitativ nicht zur Verfügung stellen kann. Der Siegeszug der Cloud lässt sich durch die fünf in Abbildung 2 ausgeführten markanten Vorteile begründen:

1. Skalierbarkeit: Unendlich verfügbare vertikale und horizontale Ressourcen
2. Innovation: Exzellenz in Qualität und Quantität der Cloud-Services
3. Servicequalität: IT als Kern der Wertschöpfung ist entsprechend aufgestellt
4. Softwareentwicklung: Entwicklungsumgebung und fachliche Services per Klick
5. Kosten: Tausch von Anschaffungskosten gegen Subskription

Qualitative und quantitative Vorteile der Nutzung von Cloud-Angeboten



Quelle: COREresearch 2021

Abbildung 2: Nutzung von Cloud bietet Vorteile in den fünf Dimensionen Skalierbarkeit, Innovation, Servicequalität, Softwareentwicklung und Kosten

Doch bedeutet die Nutzung von Cloud-Services ebenfalls, dass die Anbieter Zugriff auf die Daten der sie nutzenden Unternehmen haben und induziert damit eine neue Beurteilung von Datenschutz und Datensicherheit als es bei einem eigenverantwortlichen Betrieb der Fall ist.

Cloud-Nutzung unterstützt die Automatisierung organisatorischer Prozesse

Der technologische Fortschritt stellt Unternehmen vor die Herausforderung, die Balance zwischen moderner Infrastruktur und der Sicherheit von Daten und Informationen angemessen zum eigenen Geschäftsmodell als auch konform zur Regulierung (Gesetzgebung sowie Auslegung und Durchsetzung der Gesetze durch die Aufsicht) zu gestalten. Cloud-Ökosysteme bieten Analyse- und Maßnahmen-Tools in den Bereichen Informationssicherheit und Datenschutz an, um Anforderungen aus Compliance-Perspektive einzuhalten. Einige der Tools sind für weitere Compliance-Bereiche wie Geldwäsche-Prävention und Vermeidung von Terrorismusfinanzierung einsetzbar. Die steigenden Anforderungen an Informations- und Datensicherheit begünstigen die Technologisierung und damit Automatisierung analoger, d.h. organisatorischer Maßnahmen – diese können Hyperscaler mit einem Öko-System rund um die native Hardware besser bedienen als jeder Betreiber On-Premise. Doch bieten Cloud-Services nicht nur Chancen, sondern auch Beschränkungen in Form ihrer Regulierung:

1. Datenschutz: Datensicherheit versus betriebsnotwendige Datenteilung
2. Informationssicherheit: Datensicherheit aus der Cloud On-Premise nicht zu erreichen
3. Parallelaktion: Datenschutz ist ohne Datensicherheit nicht möglich – integriert umsetzen

Zwar kann ein Angebot aus der Cloud auch kostengünstiger als ein Betrieb On-Premise sein, jedoch ist das Kostenargument zunehmend in den Hintergrund gerückt und Eigenschaften wie Skalierbarkeit und Servicequalität sprechen mittlerweile schlagend pro Cloud. Das Versprechen der Nullerjahre „IT aus der Steckdose“ ist Realität.

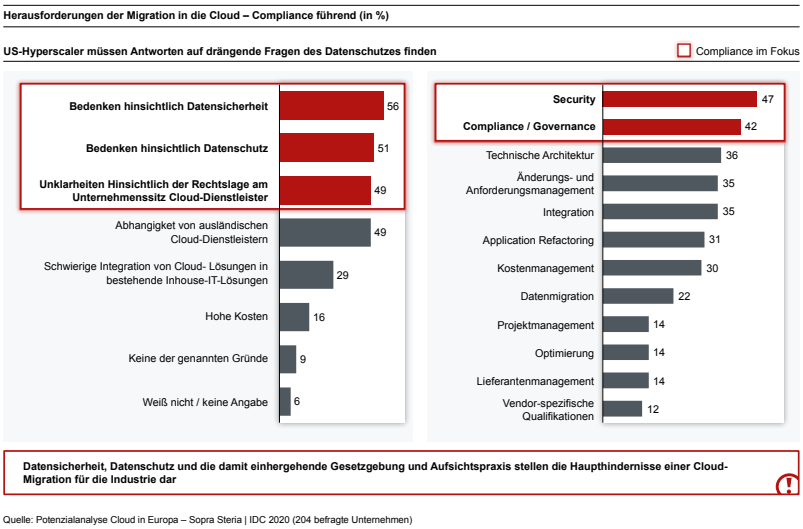


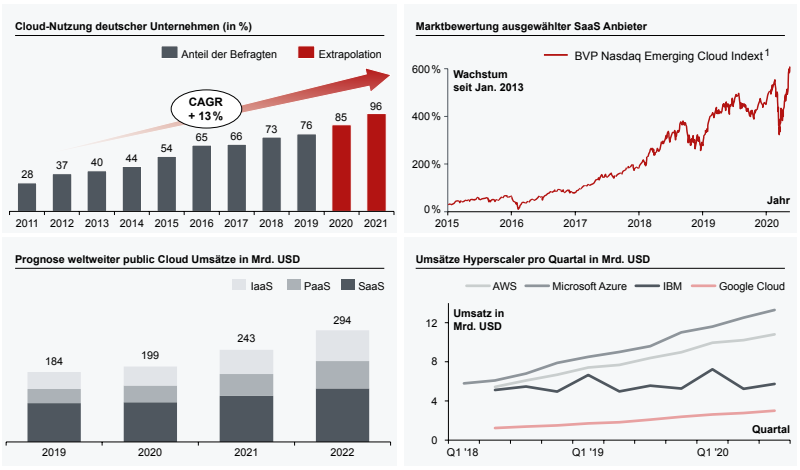
Abbildung 3: Compliance ist führende Herausforderung für Cloud-Migration

In Abbildung 3 sind die Haupthindernisse für eine Migration in die Cloud aufgeführt: Datensicherheit, Datenschutz und die mit diesen verbundenen Unklarheiten bezüglich der Rechtslage der Datenverarbeitung am Unternehmenssitz des Providers sind in zwei repräsentativen Umfragen manifest. Dabei kann eine strategisch gut vorbereitete und umgesetzte Cloud-Strategie gerade diese zwei Compliance-Gebiete umfangreich unterstützen.

2.1 Siegeszug der Cloud

Potenziale der Cloud-Nutzung sind so vielfältig, dass kein Einsatz keine Option ist

Drei von vier der befragten deutschen Unternehmen setzten 2019 bereits auf Anwendungen aus der Cloud[1]. Von den verbleibenden 24% gaben lediglich 6% der Unternehmen an, auch künftig auf die Integration und Nutzung von Cloud-Services verzichten zu wollen. Der Siegeszug der Cloud, ausgehend von 28% Cloud-Anwendungen nutzender Unternehmen im Jahr 2011, setzte sich damit bereits das zehnte Jahr in Folge eindrucksvoll fort. Es verwundert nicht, dass die Anbieter von Cloud-Dienstleistungen zu den Gewinnern der letzten Dekade gehören. Hyperscaler bauten neue Geschäftsbereiche aus dem Nichts auf, welche jeweils einen Umsatz im zweistelligen Milliardenbereich erwirtschafteten. Ähnlich beeindruckend sind die Umsatzzahlen und damit verbundenen Marktbewertungen von SaaS-Angeboten. Investitionen in solche Unternehmen wurden mit einer Vervielfachung des eingesetzten Betrages belohnt – Teilgrafik rechts oben in Abbildung 4.



1. Der BVP Nasdaq Emerging Cloud Index umfasst 52 im Nasdaq gelistete Unternehmen mit SaaS- und cloudbasierten Geschäftsmodellen Quellen: Bitcom Cloud Monitor, Yahoo Finance, Quartalsberichte Amazon, Google und IBM, Statista und Gartner

Abbildung 4: Stark steigende Cloud-Nutzung spiegelt sich in Kennzahlen und Prognosen wider

Hyperscaler bieten bessere Informationssicherheit und damit besseren Datenschutz

Diese Treiber hinter dem Siegeszug der Cloud werden durch eine stetig wachsende Anzahl an Erfolgsgeschichten über konsequente Integration von oder Migration in Cloud-Anwendungen flankiert. So geben inzwischen 78% der Cloud-nutzenden Unternehmen an, dass der Umstieg auf Cloud-Computing und die Integration der verschiedenen Anwendungsmöglichkeiten einen positiven Einfluss auf die Entwicklung des Unternehmens haben. Bereits die Hälfte der Unternehmen, die eine Cloud-Migration erfolgreich abgeschlossen haben, stellen eine Zunahme der Datensicherheit fest und nehmen somit einem der vorherrschenden Vorurteile gegenüber Cloud-Computing zunehmend den Wind aus den Segeln. Ein Viertel der Unternehmen kann bereits Bilanz ziehen und hierbei eine deutliche Reduktion der eigenen IT-Kosten feststellen[2].

[1] (Bitkom Research, KPMG, 2020)

[2] (Bitkom Research, KPMG, 2020)

Es überrascht so nicht, dass der Cloud weiterhin vielversprechende Aussichten zugeschrieben werden; das Forschungs- und Prognoseunternehmen Gartner prophezeit ein weiteres Ansteigen des Marktvolumens auf fast USD 300 Mrd. im Jahr 2022[3].

Es ist aus diesen Zahlen deutlich zu erkennen, dass Cloud-Computing Vorteile für die Anwender über Größenklassen und Industrien hinweg bietet. Die Breite des Angebotes und die Vielfältigkeit der Use-Cases für Cloud-Computing gehen mit einer Vielzahl an Motivatoren für die Cloud einher. Betrachtet man die in Studien[4,5], gegebenen Antworten auf die Frage nach den Vorteilen der Anwendung von Cloud-Computing, so lassen sich die fünf zentralen Motivatoren aus Abbildung 2 erkennen. Diese verschiedenen intendierten Effekte der Migration in oder Integration von Cloud-Angebote(n) ergeben sich dabei teils direkt, mehr noch indirekt, aus den technischen Eigenschaften und dem grundsätzlichen Wechsel von einer Lieferanten-Kunden-Beziehung hin zu einer Partnerschaft zwischen Anbieter und Nachfrager. Ein weiteres schlagendes Indiz einer „Cloud first“ Welt zeigt sich in der Tatsache, dass bestimmte Anwendungen nur noch als SaaS beziehbar sind – Beispiel Adobe Creative Cloud.

2.1.1 Skalierbarkeit als inhärentes Gestaltungsprinzip der Cloud

Skalierbarkeit technischer Infrastrukturen ist Fundament für jede Form digitaler Geschäftsmodelle

Die Verknüpfung von Skalierbarkeit und Cloud ist eine wortwörtliche. Hinter dem Wunsch nach Skalierbarkeit verbirgt sich die Hoffnung, dass sich die eigenen (digitalen) Produkte oder Dienstleistungen einer größeren Beliebtheit als ursprünglich erhofft erfreuen. Die Cloud als Infrastruktur-Ressource ist das faktische Angebot von Rechenkapazität und ermöglicht die nötige Betriebs-Ressource IT flexibel bedarfsgerecht zu beziehen. Diese Eigenschaft ist so zentral, dass sie unter dem Begriff der „rapid elasticity“ als eine essenzielle Charakteristik in der als Referenz anerkannten NIST Definition von Cloud-Computing angeführt wird[6]. Beginnend mit der Elastic Compute Cloud (EC2)[7] von Amazon wurde es 2006 ein Leichtes, IT-Ressourcen ohne weitere Interaktionen vertikal zu skalieren, mit der Containervirtualisierung war auch die rapide horizontale Skalierbarkeit einfach zu realisieren. Elastizität ist dabei mehr als nur Skalierbarkeit. Im Zeitpunkt der Normallast müssen nun nicht mehr CapEx[8] und OpEx[9] bindende Ressourcen für die wenigen Zeitpunkte der Spitzenlast vorgehalten werden. Auf den ersten Blick scheint die enorme Fluktuation der Ressourcenkonsumption eher Online-Shops, Streaming-Portale oder Nachrichtenseiten zu betreffen. Die Relevanz der Spitzenlastfähigkeit im Geschäftsmodell ist leicht zu erkennen. Doch wie der zweite Blick offenbart, kommt es auch bei anderen hochsensiblen Dienstleistungen wie z.B. Online- oder Mobile-Banking immer wieder zu einem sprunghaften Anstieg von Anfragen. Neben juristischen Konsequenzen, die ein Ausfall nach sich ziehen kann, führen diese zu empfindlichen Reputationsschäden;

[3] (Gartner, 2020)

[4] (Bitkom Research, KPMG, 2020)

[5] (IDG Research Services, 2020)

[6] (National Institute of Standards and Technology, 2011)

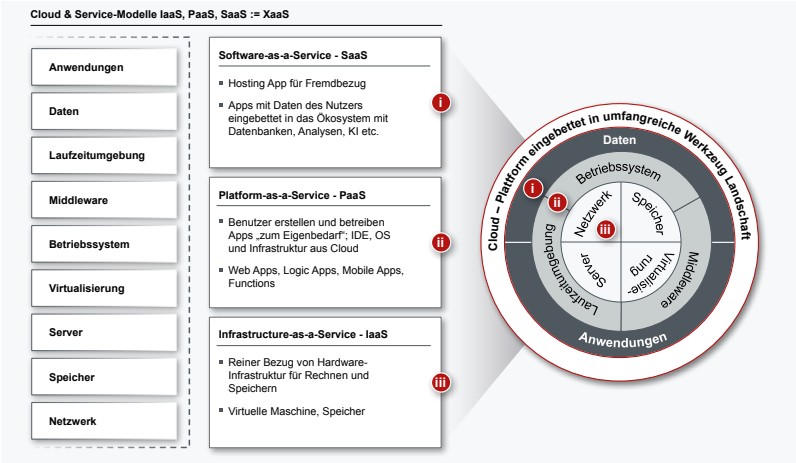
[7] (Amazon Web Services, 2006)

[8] Capital Expenditure, Investitionsausgaben

[9] Operational Expenditure; Betriebskosten

beispielsweise, wenn, wie im März 2020 geschehen, der supermaximale Ressourcenkonsum durch vermehrte Anfragen an das Online-Brokerage in Folge plötzlicher Kursstürze an den Börsen ausgelöst wird[10,11].

Die hohe Beliebtheit von Cloud-Infrastrukturen bei Start-Ups mit Internet-basierten Produkten[12] wie Netflix[13], Spotify[14], Stripe[15] oder Home24[16] ist vor allem auf diese Skalierbarkeit zurückzuführen. Für die frühe Adaption der Cloud sprach aus dem Blick der jungen Ventures der geringere CapEx und damit das geringere finanzielle Risiko, zusätzlich zur Fähigkeit, mit dem Geschäftserfolg wachsen zu können.



Quelle: COREresearch 2021

Abbildung 5: Cloud-Anbieter liefern unbegrenzte Ressourcen in den drei Modellen IaaS, PaaS, SaaS := XaaS

Bereits der Eigenbetrieb von IT stellt viele Unternehmen vor große Herausforderungen. IaaS, PaaS und SaaS – in Abbildung 5 zu XaaS zusammengefasst – stellen Hyperscaler in einer Qualitätsstufe bereit, welche die allermeisten Organisationen im Eigenbetrieb nicht abbilden können. Dieses Liefermodell XaaS stellt aber „nur" den Nukleus eines Ökosystems des Cloud-Anbieters dar, welches der Nutzer in Vielfalt und Service-Qualität nicht in Eigenleistung nachbilden kann.

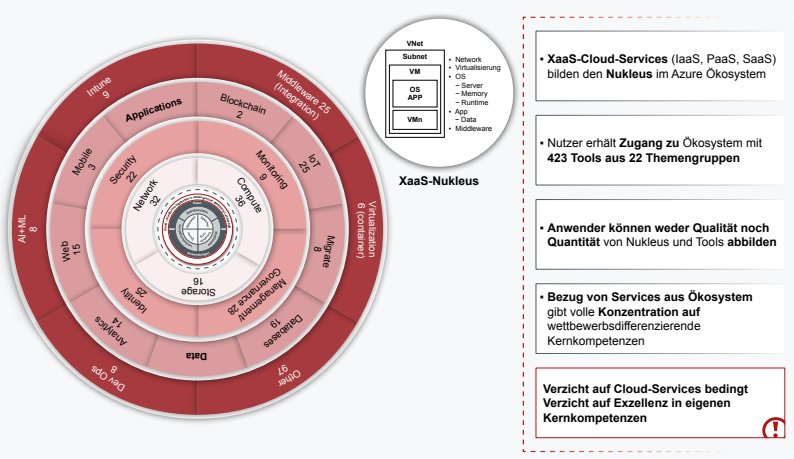
[10] (Kirchner, 2020)
[11] (@DKB.de, 2020)
[12] (Lemos, 2010)
[13] (Netflix, 2016)
[14] (Beiersmann, 2016)
[15] (Amazon Web Services, 2015)
[16] (Amazon Web Services, 2018)

2.1.2 Innovation durch Nutzung der Cloud-Ökosysteme

Der sehr naiven Vorstellung von Cloud als einem Netzwerkordner an einem tausende Kilometer entfernten Ort, stehen die auf den Webseiten der Cloud-Anbieter beworbenen Angebote wie „Analytics“, „Blockchain“, „Internet der Dinge“, „KI“ sowie „Machine Learning“ gegenüber. Es handelt sich dabei nicht um exemplarische Use-Cases, welche mit den bereitgestellten Ressourcen ermöglicht werden, sondern um tatsächlich konsumierbare Angebote. Diese komplexeren Dienstleistungen sind die logische Weiterentwicklung des initialen Angebots von Rechenleistung und Speicherplatz. Die Weiterentwicklung folgt dabei der Idee, Ergebnisse anstelle von Ware zu beziehen, und zwar – wie in der NIST Richtlinie als essenzielle Charakteristika aufgeführt – als „on-demand self-service[17]“. Exemplarisch sind in Abbildung 6 die im Azure-Universum des Cloud-Angebotes von Microsoft enthaltenen Dienstleistungen dargestellt, wie sie auch vergleichbar in den Portfolios aller anderen Hyperscaler zu finden sind.

Moderne Clouds bringen das Rechenzentrum als Commodity mit – der eigentliche Werttreiber ist das Ökosystem

XaaS (Subsumtion von IaaS+Paas+SaaS) stellt in Azure den „hardwarenahen“ Nukleus eines mächtigen Ökosystems dar



Quelle: COREresearch 2021

Abbildung 6: Lösungen und Produkte von Azure

Die Notwendigkeit des Aufbaus von Expertise und Implementierung proprietärer Anwendungen zur Erweiterung oder Ergänzung des eigenen Produktportfolios um moderne, mehrwertstiftende, doch hochkomplexe Technologien entfällt dabei.

Das Paradigma, alle nicht-geschäftsdifferenzierenden Funktionen auszulagern, greift auch hier. Exemplarisch herangezogen seien die Integration von Geldwäscheprüfungen und Chat-Bots im Banking; die gelungene Online-Banking App mit der zusätzlichen Funktionalität kann von Wettbewerbern abgrenzen, die Technologie der Spracherkennung und dahinterliegende künstliche Intelligenz kann dies nicht.

Zusätzlich zu den technischen Tools stehen auch fachliche Services zur Verfügung wie beispielsweise Check-out, Einbindung von Zahlungsdienstleistern, Warenkorbverwaltung etc. Die früher als Bibliotheken verfügbaren Funktionen sind heute fertige Applikationen. Und die Abstraktion von

[17] (National Institute of Standards and Technology, 2011)

IT-Services in der Cloud geht noch weiter: Über die Fachlichkeit hinaus stehen mächtige vorgefertigte Werkzeuge wie Künstliche Intelligenz und sogar Genomanalyse zur Verfügung. Die Moral der Geschichte: Cloud-Anwender konzentrieren sich auf ihr Kerngeschäft in Form ihrer Apps, Commodity des Liefermodells und Tools des Ökosystems liefert die Cloud.

2.1.3 Verbesserung der Servicequalität von IT-Leistungen

Die Bereitstellung von IT-Services in den drei Liefermodellen IaaS, PaaS und SaaS ist das Kerngeschäft für Hyperscaler; entsprechend müssen sie sich hier marktdifferenzierend aufstellen. Dies erfordert ein hohes Maß an Technologiekompetenz, was wiederum zu einem Vorteil für Hyperscaler führt, da Talente sich an Top Notch Technologien orientieren. Während somit für Kunden von Hyperscalern IT „nur“ eine Supportfunktion ist, ist sie für sie selbst Teil der Wertschöpfung.

Maximale Qualität von IT-Services basiert auf höchster Technologiekompetenz

Die Auffassung der IT als Kostenstelle hat in vielen Unternehmen zu einem gravierenden Schiefstand geführt. Notwendige Pflege und Wartung der Systeme werden als notwendiges Übel zu möglichst geringen Kosten durchgeführt; mit wenig überraschenden Einbußen in der Qualität der erbrachten Dienstleistung. Unter Kostengesichtspunkten ausgewählte Ressourcen werden mit einer Vielzahl kleinteiliger Aufgaben belastet und haben oft erschreckend veraltetes Betriebsmaterial zur Verfügung. Dieser betriebswirtschaftlich korrekten Auffassung von IT als Kostenstelle – es ist keine geschäftsdifferenzierende Funktion – steht das Geschäftsmodell der Cloud-Anbieter gegenüber; hier ist das Öko-System rund um „die IT“ geschäftsdifferenzierend. Die Liste des Konsums von nur der Basiskomponente „Rechenleistung“ bzw. IaaS aus der Cloud ist lang. In Abbildung 6 ist dies durch den Nukleus „XaaS“ des Cloud-Universums dargestellt und beinhaltet exemplarisch den Austausch von defekter Hardware, Konfiguration der Netzwerke, aktive Gefahrenabwehr und vieles mehr. Für einen Cloud-Anbieter sind diese Dienstleistungen bzw. deren Qualität ein Differenzierungsmerkmal gegenüber seinen Konkurrenten. Für den Cloud-Anwender ist das sowohl seine Betriebs-IT für die Produktion als auch für seine Verwaltung (Office, FiBu, HR).

Hierbei kommt vor allem die Nutzung von gemeinsamen Ressourcen zum Tragen[18]. Die Qualität einer Dienstleistung ist in erster Linie von der Kompetenz als Funktion von Wissen und Erfahrung des Dienstleisters und der Menge eingesetzter Ressourcen abhängig. Dieses Mehr an kompetenteren Ressourcen kann auf der Seite der Hyperscaler effektiv über eine Vielzahl von Kunden eingesetzt werden.

Zusätzlich ist die Automatisierung organisatorischer Maßnahmen und manueller Prozesse, welche sich in einem On-Premise Liefermodell aufgrund der zu geringen Durchlaufzahlen nicht rentiert hatten, für den Cloud-Anbieter ein lohnender Business Case; die Anwendung von technischen Prozessen ist dabei einhergehend mit der Eliminierung des menschlichen Fehlers.

Diese implizite Verschiebung der nötigen Ressourcen und Kompetenzen hin zu einem Cloud-Dienstleister reduziert bis eliminiert die Abhängigkeiten von internen Kopfmonopolen auf den Seiten der Cloud-Anwender.

[18] Essential Characteristic “Ressource Pooling”; (National Institute of Standards and Technology, 2011)

2.1.4 Nutzung der Cloud in industrieller Softwareentwicklung

Initial wirkt es kontraintuitiv, proprietäre Software auf fremden Ressourcen zu entwickeln, doch zeigen sich in der Detailbetrachtung enorme Effizienzpotentiale. Bereits in der Planung der zu erstellenden Software zeigen sich erste Unterschiede. Die nahezu unendliche Skalierbarkeit von Rechenleistung und vor allem Speicherplatz nehmen der exakten Ressourcenapproximation die Relevanz. Die Erweiterung von Serverkapazität reduziert sich von einem oft wochenlangen und aufwändigen Prozess mit den Schritten Genehmigung(en), Bestellung, Lieferung, Installation, Kommissionierung und Test zur Eingabe von einigen Kommandozeileneingaben. Am Anfang eines jeden Softwareentwicklungsprojekts steht der Aufbau der benötigten Ressourcen (Entwicklungs- und Testumgebungen) und Werkzeuge (Projektmanagement und Issue-Tracking Tools, Code-Repositories, Programme für Testautomatisierung etc.); in der Scrum Methodik oftmals als Sprint 0 bezeichnet. Die zentralen Ressourcen Speicherplatz und Rechenleistung stehen in der Form von Virtuellen Maschinen (VM) innerhalb von Minuten bereit und sämtliche Tools stehen „as a Service“ zur Verfügung.

Softwareentwicklung in der Cloud ist Konsequenz der neuen IT-Liefermodelle

Geschwindigkeitssteigerung geht dabei mit einem erheblichen Gewinn an Flexibilität der möglichen Lösungsarchitekturen einher. Stellt sich im Projektverlauf die initiale Entscheidung für einen Datenbanktyp (z.B. MySQL) als unpassend heraus, kann in wenigen Schritten eine Datenbank eines anderen Typs (z.B. PostgreSQL oder NoSQL) aus der Cloud bezogen und verprobt werden.

2.1.5 Kosteneinsparungen als ein Vorteil neben anderen

Mit der Migration des Eigenbetriebs in die Cloud werden Anschaffungskosten gegen Subskription getauscht. Die ersteren werden abgeschrieben, die zweiten nur abgesetzt.

Notwendige Aufwände für Pflege, Wartung und Überwachung der IT-Systeme müssen nicht mehr durch den Administrator vor Ort erfolgen, sondern können in fernen Datenzentren hochskalierbar durch die Experten des Cloud-Anbieters durchgeführt werden. Diese Skalierbarkeit der Personalkosten wird ergänzt um weitere kostenreduzierende Effekte wie dem zentralen Einkauf von Hardware oder der Möglichkeit, mehr Hardware auf weniger Fläche an kostengünstigeren Standorten mit oftmals dort erzeugter erneuerbarer Energie zu betreiben. Diese Skaleneffekte auf Seiten des Cloud-Anbieters werden den Gesetzen eines funktionierenden Marktes unter Wettbewerb folgend, als geringere Stückkosten an die Kunden weitergegeben.

Migration in die Cloud allein aus Kostengründen ist selten ein Case

Die Maturität der Cloud-Dienstleistungen geht auch stark mit leichteren Anwendungsmöglichkeiten einher. Die Angebote sind so auch für kleinere Organisationen ohne tieferes Expertenwissen niedrigschwellig einsetzbar. In der Cloud-Welt sind die Grenzkosten für grundlegende IT-Infrastruktur wie E-Mail, Office Applikationen etc. für ein KMU theoretisch[19] identisch wie für einen multinationalen Konzern. Die Einsparpotenziale sind folglich invariant gegen die Größe und in den Commodity-Bereichen auch unabhängig von der Branche.

[19] Cloud Anbieter geben bei Abnahme größerer Mengen oft massiv Rabatte.

2.2 Anforderungen aus der Regulatorik

In der Betrachtung über längere Zeiträume lässt sich die Akkumulation eines stärkeren Regulierungstrends[20] (siehe Abbildung 8) und der fast sprunghaften technologischen Entwicklung des Internets beobachten, welche zu einem erheblichen Mehr an zu beachtender Regulierung – Gesetze und Aufsichtsvorgaben – für die Verarbeitung von Daten geführt haben. Es ist so nicht verwunderlich, dass die Erfüllung regulatorischer Anforderungen zu großen[21], in einzelnen Branchen wie Kreditwirtschaft und Versicherungswesen (siehe Abbildung 7) zu den größten Herausforderungen[22] gehören.

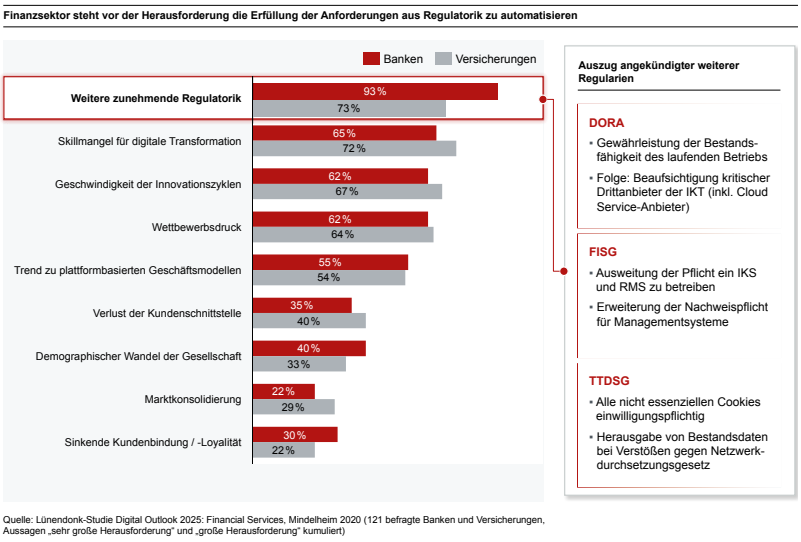


Abbildung 7: Regulatorik ist größte Herausforderung im Finanzsektor

2.2.1 Relevanz von Datenschutz auch bei Cloud-Nutzung

Unter den neuen Gesetzen, Aufsichtsvorgaben und Auslegungsentscheidungen der letzten Jahre nahm die europäische Datenschutz-Grundverordnung (DSGVO) die prominenteste Rolle ein; Datenschutz ist ein Grundrecht, dass in der Europäischen Grundrechtecharta (Art. 8) und dem deutschen Grundgesetz (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) verankert ist. Es ist somit unabdingbar, d.h. es kann nicht vertraglich außer Kraft[23] gesetzt werden. Zentrales Ziel der DSGVO ist es, die Grundrechte und -freiheiten natürlicher Personen zu schützen, insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO).

[20] Nach einem Deregulierungstrend zwischen 1980 und 2010, vgl. (Reckwitz, 2019)

[21] (Bitkom, 2020)

[22] (Lünendonk & Hossenfelder, 2020)

[23] Betroffene dürfen nur in einem seltenen Ausnahmefall (Art. 49 Abs. 1 DSGVO) auf den Schutz ihrer personenbezogenen Daten verzichten.

Whitepaper: Datenschutz nutzen – das Ende der Karenz

https://core.se/de/publications/white-paper/das-ende-der-karenz-datenschutz-nutzen

Die Auswirkungen und der Umgang mit den Anforderungen der DSGVO[24] sowohl aus der Perspektive der Anwender als auch in aufsichtlicher Praxis, sind tiefschürfend in unserem Whitepaper „Datenschutz nutzen – Das Ende der Karenz“ beschrieben. In einem kurzen Abriss stellt sich die Situation so dar, dass die DSGVO einerseits als konzeptioneller Erfolg gewertet werden kann; der US-amerikanische California Consumer Privacy Act (CCPA) in Kalifornien und weitere über 100 Datenschutzgesetze weltweit orientieren sich stark daran. Andererseits treten an anderen Stellen Widersprüche zu existierenden nationalen Gesetzen zu Tage oder bestehende Praktiken und transnationale Verträge wurden vor Gerichten als nicht vereinbar beschieden. Als Beispiele hierfür seien die Urteile auf europäischer (EuGH am 01.10.2019) und deutscher (BGH am 28.05.2020) Ebene angeführt, welche die abweichenden Vorgaben der DSGVO und dem deutschen Telemediengesetz (TMG) hinsichtlich der Einwilligung zu Cookies aufgriffen. Auch das Urteil des EuGHs vom 16. Juli 2020, dass die Übermittlung von Daten in das außereuropäische Ausland im Rahmen des Privacy Shield als nicht mit der DSGVO vereinbar feststellte, zeigt, dass noch weitere neue oder geänderte Anforderungen zu Datenschutz zu erfüllen sind.

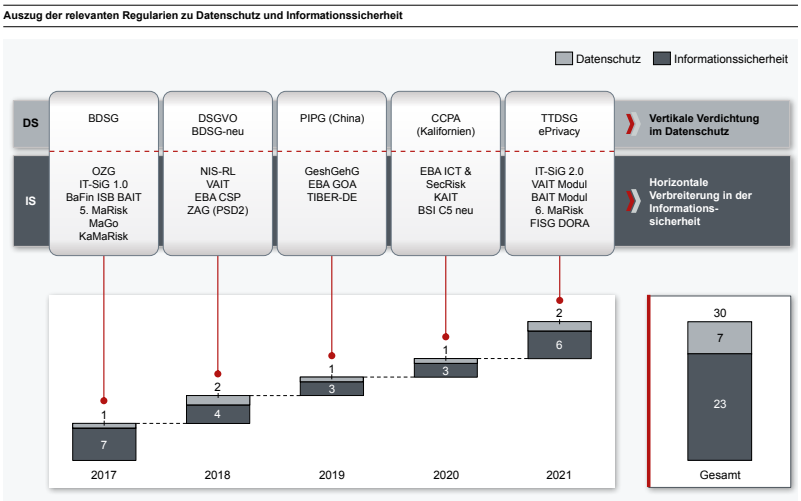


Abbildung 8: Keine Pause bei Gesetzgebung und Aufsichtspraxis in Datenschutz und Informationssicherheit

Sehr weit fortgeschritten ist die Kodifizierung der ePrivacy Verordnung, welche den Fokus auf den Schutz sämtlicher erhebbarer und damit zu schützenden Daten im Internet legt. Die nationale Umsetzung dieser Verordnung soll im Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) erfolgen, einem Artikelgesetz, das TKG und TMG zusammenführt und den zuvor aufgezeigten Dissens zur DSGVO dahingehend behebt, dass für den gewollten Zugriff des Nutzers auf Nachrichten und Telemedien eines Anbieters notwendige Informationen auf den Endgeräten des Nutzers gespeichert und abgerufen werden können. Der Bußgeldrahmen im TTDSG entspricht dem bereits bekannten aus der DSGVO.

[24] Bzw. der nationalen Kodifizierungen und Konkretisierungen, in Deutschland das neue Bundesdatenschutzgesetz (BDSG-neu) sowie Landesdatenschutzgesetze

2.2.2 Verpflichtung zur Informationssicherheit

Im Prinzip verlangen alle Regulierungen zur Informationssicherheit das Gleiche

Verpflichtende Maßnahmen der Informationssicherheit leiten sich explizit aus der europäischen NIS-Richtlinie[25] (Network Information Security) bzw. deren Umsetzung in nationalen Gesetzen ab. In Deutschland ist dies durch das IT-Sicherheitsgesetz (IT-SiG) im Jahre 2016 erfolgt. Hierin werden kritische Infrastrukturen[26] definiert, als auch deren Betreibern vorgeschrieben, IT-Sicherheit nach dem „Stand der Technik" umzusetzen und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das Gesetz umfasst zusätzlich zu den Betreibern aus den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr auch die drei Anbieterkategorien digitaler Dienste: Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste. Unter anderem müssen diese Betroffenen mindestens alle zwei Jahre die Erfüllung einer Mindest-IT-Sicherheit durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber der jeweiligen Fachaufsicht nachweisen.

Effektiver Informationsschutz erforderlich für rechtlichen Schutz

Das im April 2019 in Kraft getretene „Gesetz zum Schutz von Geschäftsgeheimnissen" (GeschGehG) regelt den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Wer sich auf ein Geschäftsgeheimnis berufen will, muss darlegen können, dass Geschäftsgeheimnisse durch angemessene Sicherheitsmaßnahmen geschützt sind. Ein effektiver Informationsschutz trägt somit nicht nur technisch-organisatorisch, sondern auch rechtlich zum Geheimschutz bei.

Eine regulatorische Mindest-IT-Sicherheit ist der im Jahr 2016 durch das BSI mit Blick auf die Cloud entwickelte Cloud Computing Compliance Criteria Catalogue (C5)[27]. C5 basiert auf international anerkannten IT-Sicherheitsstandards wie ISO 27001[28], der Cloud Security Alliance Cloud Controls Matrix 3.0.1 und den BSI-eigenen IT-Grundschutz-Katalogen. Er bildet eine verbindliche Mindestgrundlage für die Cloud-Sicherheit und den Einsatz von Public Cloud-Lösungen. Vorrangig gilt dieser geprüfte Standard für deutsche Regierungsbehörden und Organisationen, die mit der Regierung zusammenarbeiten, jedoch wird C5 auch zunehmend von der Privatwirtschaft als Voraussetzung herangezogen.

Branchenspezifisch sind die Unternehmen der Kreditwirtschaft (KWG) und Versicherungen (VAG) verpflichtet durch eine angemessene technisch-organisatorische Ausstattung die Einhaltung ihrer jeweiligen Spezialvorschriften zu gewährleisten. In den Spezifikationen Bankaufsichtliche Anforderungen an die IT (BAIT)[29] bzw. Versicherungsaufsichtliche Anforderungen an die IT (VAIT)[30] und Kapitalverwaltungsaufsichtliche

[25] (Amtsblatt der Europäischen Union, 2016)

[26] Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (Bundesministerium des Innern, 2009))

[27] (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)

[28] (ISO (International Organization for Standardization), 2013)

[29] (Bundesanstalt für Finanzdienstleistungsaufsicht, 2018)

[30] (Bundesanstalt für Finanzdienstleistungsaufsicht, 2019)

Anforderungen an die IT (KAIT)[31] der BaFin ist jeweils ein Informationssicherheitsmanagement explizit gefordert. Die BAIT in der Fassung 2021[32] wird um zwei Module „Kundenbeziehungen mit Zahlungsdienstnutzern“ und „Kritische Infrastrukturen“ erweitert. Das erste Modul wurde zuvor als Rundschreiben „Zahlungsdiensteaufsichtliche Anforderungen an die IT“ (ZAIT) konsultiert.

DORA ist der radikale Versuch der Komplexitätsreduktion

Ergänzend dazu wurde am 24. September 2020 ein Entwurf der Europäischen Kommission veröffentlicht: Digital Operational Resilience Act (DORA)[33]. Dieser fasst mehrere EU-Initiativen verschiedener Institutionen zusammen (siehe Abbildung 9) und soll eine Grundlage für Finanzregulierungs- und -aufsichtsbehörden dienen. Bisher wurden Unternehmen des Finanzsektors vorrangig auf ihre finanzielle Stabilität geprüft. DORA soll nun auch die Gewährleistung der Bestandsfähigkeit des laufenden Betriebs sicherstellen. Für die Praxis heißt dies zusätzliche und einheitliche Anforderungen an IT-Sicherheits- und Risikomanagement in allen Finanzdienstleistungssektoren. Indirekt folgt daraus die Beaufsichtigung von kritischen Drittanbietern der Informations- und Kommunikationstechnik, welches Cloud Service-Anbieter miteinschließt. Damit wird das Vorgehen dem der Datenschutzaufsichtsbehörden angeglichen. Konkret müssen erstens Finanzdienstleister einen Nachweis über die Angemessenheit ihrer Sicherheitsmaßnahmen führen, dieses Reporting kann als Cloud-Service effizient organisiert sein. Zweitens können Aufsichtsbehörden die Performanz verschiedener Finanzdienstleister direkter vergleichen, was mehr Durchgriff, höhere Anforderungen und weniger Möglichkeiten für Ausreden impliziert. Drittens können Cloud-Anbieter einheitliche Services auf Basis dieser Standards bieten, was wiederum das Potential für Auslagerungen erhöht, da standardisiertes Geschäft kein Kerngeschäft der Finanzdienstleister ist und in der Cloud skaliert werden kann.

Datenschutz ist ohne Informationssicherheit nicht zu erreichen

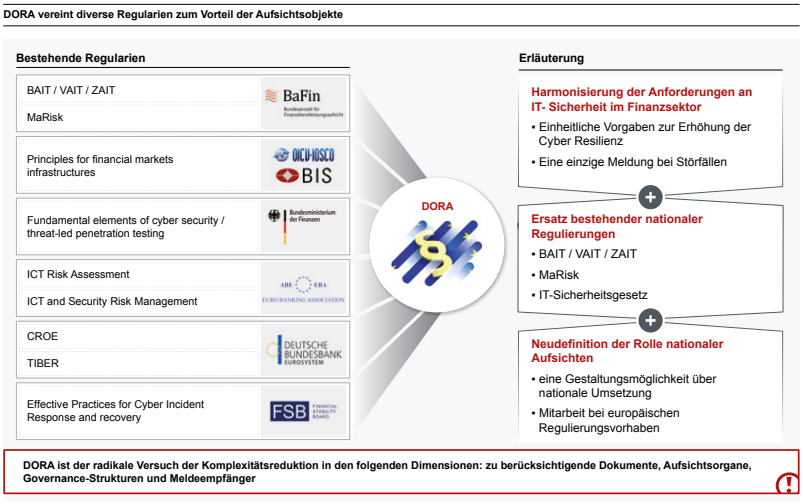


Abbildung 9: Harmonisierung der Informationssicherheit in Europa durch DORA

[31] (Bundesanstalt für Finanzdienstleistungsaufsicht, 2019)

[32] (Bundesanstalt für Finanzdienstleistungsaufsicht (BAIT), 2020)

[33] (Europäische Kommission, 2020)

Die Umsetzung der Gesetze im organisatorischen als auch technischen Sinne legt nahe, ein Informationssicherheit-Managementsystem (ISMS) zu etablieren und im besten Falle nach dem oben erwähnten Standard ISO 27001 zu zertifizieren, da so angemessene Sicherheitsmaßnahmen nach außen dokumentiert werden. Im Allgemeinen ist eine solche Zertifizierung für Unternehmen nicht verpflichtend, für Versicherungen und Finanzdienstleister jedoch explizit durch die BaFin empfohlen.

Weitere geplante Vorhaben wie die Verpflichtung aus dem Onlinezugangsgesetz (OZG) bis Ende 2022 mit dem Ziel Verwaltungsleistungen von Bund und Ländern auch elektronisch über Verwaltungsportale nutzbar zu machen werden Digitalisierungsbedarfe weiter erhöhen.

2.2.3 Verknüpfung von Datenschutz und Informationssicherheit

Datenschutz und Informationssicherheit werden oft synonym verstanden, doch sind dies in der Praxis getrennte Sphären – freilich mit Überschneidungen. Diese Trennung mag einerseits in der Unbedingtheit von Datenschutz im Gegensatz zur für viele Wirtschaftsteilnehmer bedingten bzw. freiwilligen Umsetzung von Informationssicherheit begründet sein. Hieraus haben sich Best-Practices im Datenschutz in Organisationen, welche keine Maßnahmen der Informationssicherheit treffen müssen, entwickelt. Eine weitere Ursache sind die unterschiedlichen Abwehrrichtungen: Während Datenschutz personenbezogene Daten von natürlichen Personen gegen unrechtmäßige Verarbeitung durch Wirtschaft und Verwaltung schützt, verhindert Informationssicherheit den unberechtigten Zugriff durch interne wie externe Angreifer auf jegliche Art von in der Organisation vorhandenen Informationen. Schon anhand der Definition der personenbezogenen Daten als „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen“[34], jedoch spätestens in der technischen Umsetzung wird deutlich, dass Informationssicherheit und Datenschutz bei dem Schutz personenbezogener Daten zwei Seiten derselben Medaille sind. In der Informationssicherheit obliegt die Feststellung, ob ein Zugriff berechtigt oder nicht berechtigt ist, dem Inhaber der Informationen, im Datenschutz ist diese per Gesetz vorgegeben. Die technisch-organisatorischen Maßnahmen, um den unberechtigten Zugriff auf Informationen und den Schutz der personenbezogenen Daten im Sinne der Informationssicherheit zu verhindern, sind dabei deckungsgleich[35].

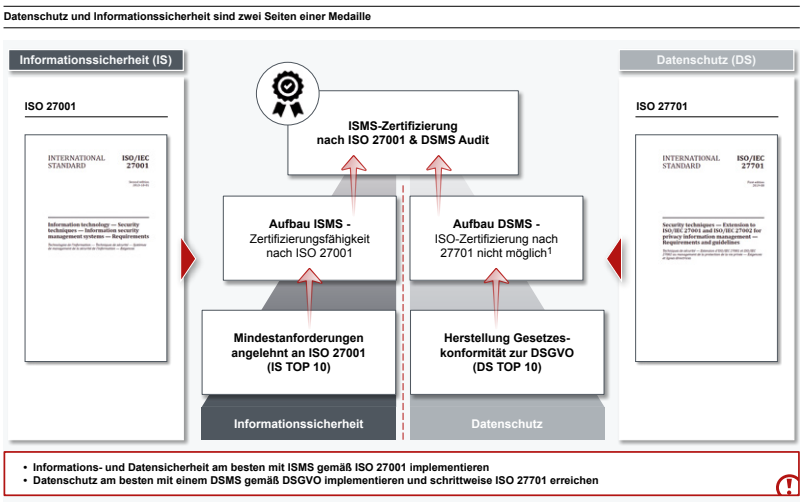
TOM sind das Scharnier zwischen Informationssicherheit und Datenschutz

Man kann diese in Abbildung 10 illustrierten Zusammenhänge an den Überschneidungen zwischen dem ISO-Standard 27001 für Informationssicherheitsmanagementsysteme (ISMS) und dem ISO-Standard 27701 für Datenschutz erkennen. Aufbau, Betrieb, Prüfung und Verbesserung eines ISMS nach ISO 27001 ist ein sowohl von Wirtschaft als auch Regulatoren anerkanntes Vorgehen und eine Zertifizierung kann eine Organisation von weiteren Nachweisen adäquater Maßnahmen zur Informationssicherheit entbinden. Dagegen steht zum ISO-Standard 27701 kein Zertifizierungsregime zur Verfügung, d.h. eine „DSGVO-Zertifizierung“ gemäß Art. 42 DSGVO[36] ist nicht möglich.

[34] (Bundesanstalt für Finanzdienstleistungsaufsicht, 2019)

[35] (Bundesanstalt für Finanzdienstleistungsaufsicht (BAIT), 2020)

[36] (Europäische Kommission, 2020)



Quelle: COREresearch 2021

Abbildung 10: ISO-Standard 27701 ist nicht zu empfehlen

Datenschutz am besten über ISMS nach ISO 27001 zu erreichen – ISO 27701 nicht zu empfehlen

Beide Managementsysteme adressieren mit einem identischen Aufbau die gleiche Aufstellung in Infrastruktur, Organisation, Personal und Compliance und sollten somit konzeptionell zusammen betrachtet werden. Insgesamt wurden 39 Änderungen am ISO 27001 vorgenommen, um ihn zum ISO 27701-Standard zu erweitern. Diese Änderungen können mit 20 IS-Artefakten und neun DS-Artefakten umgesetzt werden. Dieses Vorgehen der Standarderweiterung birgt ein großes Problem: Ein Standard für Informationssicherheit (der von Informations- /IT-Sicherheitsexperten entwickelt wurde) kann nicht linear auf Datenschutz übertragen werden, da dieser der Datenschutz-Grundverordnung genügen muss. Dies scheint das Standardisierungsgremium am Ende auch verstanden zu haben, weswegen noch zwei Anhänge an den normativen Teil des Standards „angeschraubt“ wurden, um der DSGVO, d.h. ihrem spezifischen Vokabular und vor allem ihren Grundprinzipien und Pflichtdokumenten Genüge zu tun. Zusammengefasst bedeutet das, dass zur Erfüllung des ISO 27701-Standards zusätzlich zum Aufbau eines adäquaten ISMS die 39 Datenschutz-Erweiterungen erfüllt sein und dann noch darüberhinausgehend alle Anforderungen der DSGVO gemäß der Rolle des Unternehmens – Verantwortlicher (Anhang 1) und/oder Auftragsverarbeiter (Anhang 2) – umgesetzt werden müssen. Der direkte Aufbau eines solchen DSMS stellt sich so als sehr ambitioniertes Unterfangen mit begrenztem Nutzen – aufgrund der fehlenden Zertifizierungsfähigkeit und damit einhergehenden erleichterten Kommunikation von Compliance – dar. In Anbetracht der unbedingten Anforderungen der DSGVO empfiehlt sich daher am besten parallel zur Herstellung der DSGVO-Konformität der Aufbau eines ISMS gemäß ISO 27001-Standard. In Abbildung 10 wird ein dreistufiger Weg für beide Managementsysteme ISMS und DSMS vom Basisschutz über Zertifizierungsfähigkeit bis zur Zertifizierung respektive Auditierung im Falle von Datenschutz skizziert.

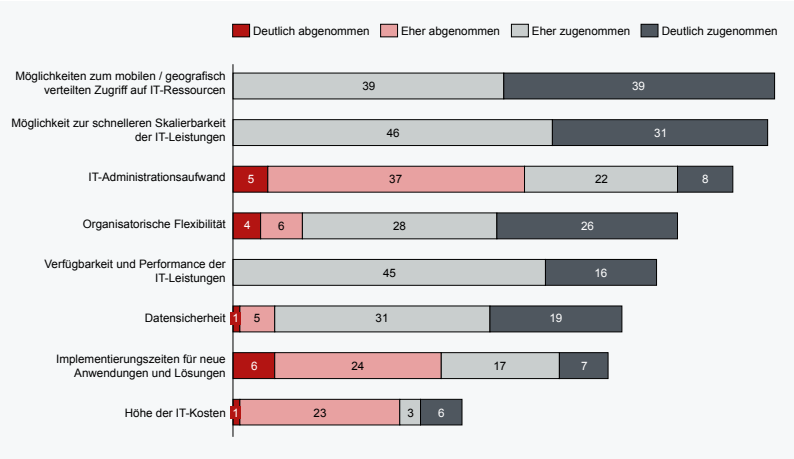
3 Cloud überfordert alle Stakeholder – gefährliches Halbwissen führt zu suboptimalen Lösungsmustern

Viele Wege führen in die Cloud, werden jedoch viel zu häufig nicht beschritten. Die Gründe sind vielfältig: Skepsis gegenüber Cloud Computing aus Unwissenheit zu Qualität und Quantität moderner Cloud-Angebote, gefühlte Unsicherheit eines „Machtverlustes“ über die eigenen Daten, die zeitliche und inhaltliche Diskrepanz zwischen Regulierung und einsatzreifen Technologien, fehlende Digitalisierungskompetenzen in Organisationsstrukturen oder es wird schlicht und ergreifend jede Änderung als Störenfried zum Status Quo wahrgenommen.

3.1 Cloud zwischen Wahrnehmung und Realität

Gefühlte Wahrheiten sind wirkmächtiger als rationales Wissen – ‚Fühlen schlägt Denken‘. In Zeiten postfaktischer Verunsicherung genügen Fake News, um aus gefühlter Unsicherheit emotional getrieben zu handlungsleitenden Feststellungen zu gelangen. Der kühl kalkulierende Homo oeconomicus ist die meiste Zeit eine Mär; Konsumentscheidungen etwa werden allen rationalen Bemühungen zum Trotz vornehmlich emotional getroffen. Erstaunlich hingegen ist, dass dieses altbekannte Prinzip auch bei der Entscheidung für oder gegen die Cloud durch gut ausgebildete und erfahrene Führungskräfte schlägt. In allen entscheidenden Aspekten bietet die Cloud Vorteile (siehe Abbildung 11), trotzdem halten sich Vorurteile hartnäckig. So halten aktuell etwa nur 40% der Entscheidungsträger deutscher Banken die Cloud für sicher[37]. Bestärkt werden sie in ihrer Sicht der Dinge durch Ereignisse wie den Fall des EU/US Privacy Shield oder den Vorstoß des Gesetzgebers zur strukturellen Schwächung starker Kryptografie als Maßnahme zur Terrorabwehr via Zugriff auf kryptografische Schlüssel.

Wahrgenommene Effekte der Cloud-Migration in deutschen Unternehmen (in %)



Quelle: (Bitkom Research, KPMG, 2020)

Abbildung 11: Vorteile der Migration in die Cloud zeigen sich auf allen Kosten- und Wertbeiträgen

[37] (Francke, 2020)

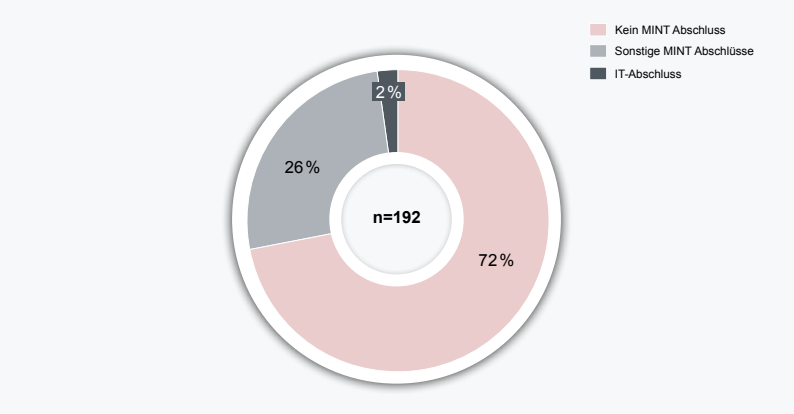
Mit dieser Skepsis werden Unternehmen die Chancen einer Cloud-Migration nicht für sich nutzen können. Hier genügt oft das unbestimmte Gefühl, die Verwahrung der Daten im Rechenzentrum im eigenen Keller sei sicherer, weil besser vor unbefugtem Zugriff geschützt. Damit einher geht die Angst, in der Cloud verwahrte Daten wanderten unweigerlich in die USA und würden dortigen Geheimdiensten und Wettbewerbern offenbart. Als Folge stellt sich das Gefühl ein, mit Herausgabe der eigenen Daten in eine Cloud auch die Kontrolle über die Daten abzugeben. Ähnlich gelagert ist die Befürchtung, durch Aufgeben der eigenen Infrastruktur Unabhängigkeit einzubüßen sowie langfristig Zugang zu wettbewerbsrelevantem IT-Know-how zu verlieren.

Anbieterabhängigkeit ist mit Containerisierung, Exit-Szenario und Wahrung der Datenübertragbarkeit beherrschbar

Dabei halten diese Vorurteile einer gelassen-rationalen Überprüfung kaum stand. Mittlerweile stehen Werkzeuge und Methoden zur Verfügung, die in der Cloud eine sichere Datenhaltung gewährleisten (siehe Kapitel 4). Cloud-agnostische Plattformen wie Kubernetes reduzieren die Gefahr eines Vendor Lock-Ins, da sich auf ihnen betriebene Systeme mit geringem Aufwand zwischen Anbietern portieren lassen. Gleichzeitig wächst die Verfügbarkeit des erforderlichen Know-hows exponentiell, analog zur Verbreitung der Technologie, während das zum Betrieb eigener Miniatur-Infrastrukturen erforderliche Wissen proportional teurer zur Verfügung gehalten werden muss.

Darüber hinaus ist anzumerken, dass neben den gefühlten Risiken des Machtverlustes über eigene Daten und Infrastruktur die ganz reale Bedrohung aus mangelnder Informationssicherheit tritt. Eine Gegenüberstellung mehrerer hundert Personen starker, rund um die Uhr mit Penetration-Tests, Absicherung, Monitoring und Abwehr beschäftigter Security-Abteilungen großer Cloud-Anbieter mit den vergleichsweise dürftigen Pendants auf Seiten der Cloud-Skeptiker führt vor Augen, wo tatsächliche Gefahren lauern. Zudem ist zur Kenntnis zu nehmen, dass auch der Betrieb On-Premise unter Wirtschaftlichkeitsaspekten nicht ohne Entwicklungsplattformen, Test- und Laufzeitumgebungen auskommt, bei welchen es sich sehr häufig ebenfalls um US-amerikanische Produkte handelt. Selbst Open Source Software wird nahezu ausnahmslos auf der Infrastruktur amerikanischer Organisationen entwickelt wie Apache, Red Hat oder Free Software Foundation, welche gleichfalls den Anordnungen der US-Geheimdienste Folge leisten müssen.

Anteil der MINT Absolventen bei DAX-Vorständen



Quelle: COREresearch 2021 | Stand Februar 2021

Abbildung 12: MINT-Kompetenz ist in DAX-Vorständen unterrepräsentiert.

Auch noch 15 Jahre nachdem Amazon mit Amazon Web Services (AWS) Cloud-Computing für Unternehmen massentauglich machte, beherrschen viele Unternehmen respektive deren Unternehmensführungen die Disziplin Cloud-Computing nicht oder nur unzureichend. Fehlende Cloud-Kenntnisse in Technologie, Regulatorik und Aufsicht oder das vorherrschende Unbehagen der Verantwortlichen resultieren in verzögerter oder gänzlich ausbleibender Erschließung der Einsatzmöglichkeiten der Cloud.

MINT-Know-how in DAX-Vorständen zu wenig ausgeprägt

Die blinden Flecken beginnen hierbei oft schon bei den grundlegenden Fragen nach den zu erschließenden Synergiepotenzialen oder den konkreten Einsatzmöglichkeiten über den reinen Onlinespeicher historischer Cloud-Angebote hinaus und setzen sich fort bei der Fragestellung nach dem passenden Cloud-Konzept und den Vor- und Nachteilen zwischen Public und Private Cloud-Lösungen. Maßgeblich verantwortlich hierfür ist nicht zuletzt die vorherrschende Gegensätzlichkeit von Anforderungen an Expertise und Governance zur Aufrechterhaltung eines komplexen Status quo und den erforderlichen Kenntnissen und Mindsets zur Transformation und kontinuierlichen Weiterentwicklung des Unternehmens in einem Umfeld, in dem IT zunehmend zu einem, wenn nicht sogar dem entscheidenden Faktor für eine erfolgreiche Unternehmensausrichtung wird.

So sehen traditionelle Kompetenzprofile für die Zusammensetzung eines Konzernvorstandes in der Regel Führungserfahrung, die Vertrautheit mit dem entsprechenden industriellen Sektor und der damit verbundenen Wertschöpfungsketten, Kenntnisse zu finanzrechtlichen Themen wie Bilanzierung, Rechnungswesen, Recht, Compliance und Abschlussprüfung, ausgeprägte Erfahrungen in den Gebieten Personal, Gesellschaft, Kommunikation und Medien sowie Allgemeinkenntnisse aus sektorübergreifenden Wirtschaftsbereichen vor. Anforderungen an ausgeprägte Erfahrungen in den Bereichen Digitalisierung und Informationstechnologie oder agile Methoden zur Produkt- und Unternehmensentwicklung komplettieren das dargestellte Kompetenzprofil für die Zusammensetzung des Konzernvorstandes in vielen Unternehmen erst seit Kurzem oder noch überhaupt nicht. Immerhin beträgt, Stand Februar 2021, der Ausbildungsabschluss in einem MINT-Fach 28% aller Vorstandsposten im DAX (Abbildung 12).

Hierbei liegt die Ableitung nahe, dass der Stellenwert spezifischer Kompetenzen bei Zusammensetzung des Konzernvorstandes sich auch auf die Gewichtung eben dieser Disziplinen bei organisatorischer und personeller Ausgestaltung der darunterliegenden Ebenen auswirkt.

Verkompliziert wird die Entscheidung zu einer Erweiterung von Personal und Strategie um die Kernkompetenzen Technologie und Digitalisierung durch den oft komplexen Status quo der IT-Infrastruktur des Unternehmens. Der in der Regel vorherrschende Wunsch nach einer agilen und technologieorientieren Unternehmensausrichtung wird überstimmt durch das Bedürfnis nach einer Absicherung des bereits Erreichten.

Resultat fehlender Expertise ist nicht selten das Aufgreifen weit verbreiteter Vorurteile gegenüber Cloud-Computing in den Themenkomplexen Daten- und Informationssicherheit, Integrations- und Wartungskosten, Administrationsaufwand, Verfügbarkeit, Performanz und Integrationsfähigkeit in bestehende IT-Infrastrukturen; meist kombiniert mit der Sorge vor der Abhängigkeit von einem Cloud-Provider, dem sogenannten Vendor Lock-In.

Letztendlich muss die Frage erlaubt sein, ob Gefühl und Unwissen die besseren Ratgeber als Fakten und Know-how sind, um die immensen Vorteile der Cloud links liegen zu lassen.

3.2 Entwicklung zwischen Regulierung und Technologie

Regulatorische Vorgaben wie europäische Verordnungen, nationale Gesetze und Auslegungen der Aufsichtsbehörden laufen der technischen Entwicklung hinterher. Das ist nicht neu und auch gut so, denn sonst stünde es schlecht um den technischen Barwert unseres Wohlstandes. Allerdings darf dieser zeitliche Abstand zwischen dem praktizierten Stand der Technik und dessen Regulierung nicht zu groß werden, sonst verliert der Regulator „den Sichtkontakt“ zur Technologie, die er als Gesetzgeber mit klugen Gesetzen und als Aufsicht mit geschäftsnahen Aufsichtspraktiken in ihren Gefahren einhegen und in ihren Chancen entfesseln will.

Mangelnde Adäquatheit der regulatorischen zur technologischen Entwicklung verschenkt immense Potenziale

Im Ergebnis ist der Stand der regulatorischen Entwicklung nicht adäquat zum Stand der Technik einsatzreifer Technologie. Allein an der Entstehungsdauer von EU-Gesetzen und der von Standards im Internet wird das unterschiedliche Tempo sichtbar: Während EU-Regularien im Durchschnitt in 19 Monaten entstehen, benötigen Internet-Standards in ihrer Entstehung im Schnitt 1,5 Monate. Hinzu kommt die in Kapitel 2.2 dargelegte Zunahme von Regelungen in ihrer Anzahl. Diesem Zeitverlust immanent ist dann die fehlgeleitete Aufsicht über das „verspätete“ Gesetz. Diese nimmt den bereits verspäteten gesetzgeberischen Faden auf und gibt den Zeitverlust als „Regulatorische Schulden“ (analog zu Technologischen Schulden) weiter. Technologische Schulden sind endogen; sie resultieren aus der Bewertung der im Einsatz befindlichen Technologien zwischen „Legacy“ und „Stand der Technik“ und beschreiben die Ergebniseinbußen durch Nutzung einer nicht dem Stand der Technik entsprechenden Technologie.

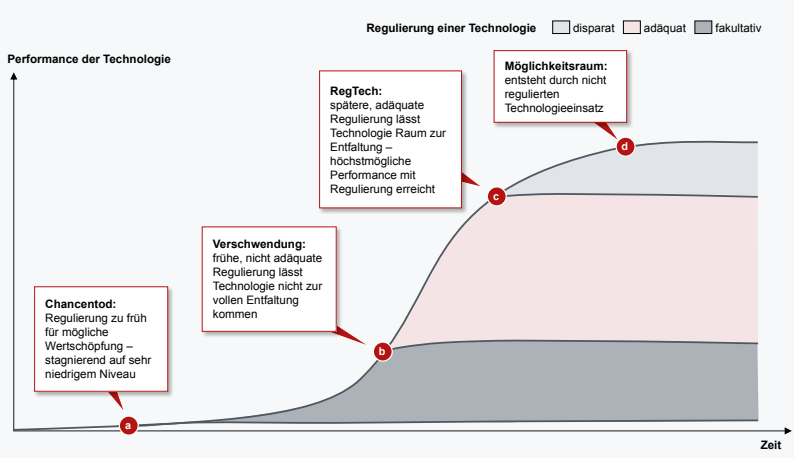
Regulatorische Schulden sind exogen; sie entstehen, wenn eine einsatzreife Technik zum Zeitpunkt ihrer Einsatzfähigkeit nicht adäquat[38] reguliert ist. Sie wirken sich in Abhängigkeit des Zeitpunktes einer Regulierung wie in Abbildung 13 illustriert unterschiedlich aus. Greifen Gesetzgeber und/oder Aufsicht zu früh (Segment a in der Abbildung) in eine sich noch entwickelnde Technologie ein und/oder nicht adäquat zu einer gegebenen Technologie (b), wird das gesamte Potenzial dieser Technologie für die Wertschöpfung des Unternehmens und der Gesellschaft verspielt. Einzig zu diesem Zeitpunkt ist eine Lobbyarbeit zur Ermöglichung und Unterstützung der Technologie sinnvoll. Diese Lobbyarbeit trägt auch dazu bei, einer später einsetzenden und adäquaten Regulierung (c) mit optimalem Interessensausgleich im Sinne einer Technikfolgenabschätzung den Weg zu bereiten. Einen Sonderfall stellt eine nicht regulierte neue Technologie

[38] Adäquat ist eine Regulierung, wenn sie einen relevanten und einsatzreifen Stand der Technik vollständig, konsistent, überschneidungsfrei und verständlich regelt.

dar (d), denn ihr Einsatz kann so den größten Beitrag zu einem Ergebnis liefern. Es gilt hier der Grundsatz, dass gar keine Regulierung keinerlei Beschränkung und somit den größtmöglichen Ergebnisbeitrag im Vergleich zu einer mit der Verfügbarkeit zeitgleich gültigen adäquaten Regulierung bedeutet.

Adäquate Regulierung lässt Technologie sich entfalten und induziert Wettbewerb unter fairen Bedingungen

Regulierung birgt regulatorische/rechtliche Risiken für die Hebung von Potenzialen aus Technologie



Quelle: COREresearch 2021

Abbildung 13: Illustration von regulatorischen Schulden als Ursache von Minderergebnissen

Verharrt das techno-regulatorische System in den Segmenten a und b, erzeugt das beispielsweise Unsicherheit bei potenziellen Anwendern („Aufsicht wird das ohnehin nicht genehmigen oder sofort verbieten“), einen suboptimalen Technologieeinsatz durch Zwang zum eigenverantwortlichen Einsatz von dann suboptimaler IT, Einschränkungen der digitalen Aktivitäten und Weiterentwicklungen und damit verspäteten oder gar ausbleibenden Produktinnovation bei der Weiterentwicklung von Geschäftsmodellen und Wertschöpfungsketten. Währenddessen werden Wettbewerber außerhalb der EU nicht in gleichem Maße gelähmt, was den Druck zusätzlich erhöht.

Resultate der mangelnden Adäquatheit zwischen regulatorischer und technologischer Entwicklung sind zu große Interpretationsspielräume, Unsicherheit und Todschlagargumente gegen neue Technologien, die letztendlich den Entscheidungsprozess stören. Dies führt zu verspäteter oder gar keiner Nutzung neuer Technologien, was Unternehmen vom technischen Fortschritt entkoppelt, den mit besserer Regulierung versehene Wettbewerber nutzen.

Als Beispiel sei das EU/US Privacy Shield genannt: Der Stand der Technik in Form von arbeitsteiliger Datenverarbeitung in den USA wird eingesetzt, die regulatorischen Risiken der gegenwärtigen nicht adäquaten Regulierung und der zukünftigen Nicht-Konformität wurden akzeptiert. Mit dem EuGH-Entscheid „Schrems II“ aus dem Juli 2020 offenbart sich nun das Risiko des faktischen Verbots der Nutzung einer erprobten und langjährig bewährten Technologie.

EU/US Privacy Shield

Abseits der allgemeinen Schutzmechanismen der Cloud-Anbieter muss angemerkt werden, dass wie in Kapitel 2 bereits erwähnt, mit dem Schrems II Urteil des EuGH das Privacy Shield Abkommen zwischen der EU und der USA außer Kraft gesetzt wurde und sich dadurch eine schwer lösbare politische Grundsatzfrage bei der Nutzung von Clouds ergibt, nämlich wenn es um Zugriffsbefugnisse von Sicherheitsbehörden geht. Das Abkommen bietet nach diesem Urteil keine gültige Grundlage mehr für die Übermittlung und Verarbeitung personenbezogener Daten von EU-Bürgern zu bzw. durch US-Unternehmen (insb. auf US-Servern).

Bei der Frage der Übermittlung personenbezogener Daten ist dabei vorrangig auf den Standort der Daten abzustellen. Deshalb sind bei US-Unternehmen Server-Standorte innerhalb der EU empfehlenswert und sollten nach Möglichkeit vertraglich vereinbart werden. Jedoch darf nicht außer Acht gelassen werden, dass US-Unternehmen trotzdem ihrem nationalen Recht unterliegen und verpflichtet sind bei Anfragen der US-Sicherheitsbehörden auch personenbezogene Daten herauszugeben. Vor dem Hintergrund Schrems II stellt es also ebenfalls keine absolute Lösung dar, sondern nur im Zusammenhang mit anderen Vorkehrungen.

Ohne ein neues Abkommen müssen folglich die jeweils Daten-exportierenden Unternehmen selbst prüfen und sicherstellen, dass ein der Sache nach gleichwertiges Datenschutzniveau gewährleistet wird. Dies ist vor allem mithilfe von Standardvertragsklauseln in Kombination mit zusätzlichen Garantien und Maßnahmen (z. B. Verschlüsselung, Anonymisierung, vertraglich vereinbarte Garantien für Betroffene etc.) möglich. Die EU-Kommission hat kürzlich einen neuen Entwurf der Standardvertragsklauseln veröffentlicht und zur Diskussion gestellt. Derzeit ist jedoch noch unklar ob und wann dieser neue Entwurf verabschiedet wird und verwendet werden kann sowie ob dieser geeignet ist die Problematik von Zugriffsmöglichkeiten seitens Sicherheitsbehörden datenschutzkonform zu adressieren. Daher gilt es die Entwicklungen auf regulatorischer und politischer Ebene weiterhin im Blick zu haben.

3.3 Trend zur Multicloud-Nutzung

Vorzüge und Herausforderungen des Einsatzes von Cloud-Angeboten können gleichermaßen mit dem parallelen Einsatz der Cloud-Services von mehr als nur einem Anbieter skalieren. Hierbei ist es den wenigsten Unternehmen möglich, bei bewusster oder unbewusster Gestaltung ihrer Cloud-Architektur auf die Inanspruchnahme von nur einem einzigen Cloud-Anbieter zu setzen. Sukzessive werden Anwendungen, die in der Vergangenheit tief in den eigenen IT-Systemen der Unternehmen integriert waren, seitens der Service-Provider in die Cloud verlagert. Die Wahl der Cloud-Infrastruktur wird in diesem Szenario durch die Provider getroffen und resultiert je nach Komplexität der ursprünglichen Anwendungslandschaft in einem Architekturbild mit einer Vielzahl an Cloud-Anbietern.

Realität zwingt Unternehmen zur parallelen Nutzung mehrerer Cloud-Anbieter

Multicloud-Vorgehen ermöglichen gleichzeitig aber auch eine providerübergreifende Auswahl von Cloud-Angeboten entsprechend der individuellen Bedürfnisse des eigenen Unternehmens und sind insbesondere dank der verbreiteten Nutzung von Workplace-Angeboten aus der Cloud, bspw. von Microsoft, zu einem industrieübergreifenden Standard geworden. In der IT- und Cloud-Architektur der Unternehmen trifft Azure als Cloud für die Workplace-Anwendungen von Microsoft hierbei häufig auf die Clouds von Amazon Web Services, Google Cloud Platform, SAP, Salesforce oder IBM. Als Konsequenz hieraus setzen bereits heute acht von zehn Unternehmen in ihrer Zielarchitektur auf mehr als einen Cloud-Provider.[39] Oft auch in der Absicht, einen Vendor Lock-In zu vermeiden, sich also dem Bestreben der Provider entgegenzustellen, Kunden einzig und allein an die eigenen Services zu binden.

Die Anforderungen an einen erfolgreichen Einsatz von Cloud-Angeboten potenzieren sich hierbei durch den Zugriff auf jeden weiteren Cloud-Provider. Unternehmen benötigen Experten mit Kenntnissen zu allen eingesetzten Cloud-Technologien für ein effizientes Management von Zugriffen, Benutzern und Projekten, vor allem jedoch auch für die Gewährleistung der in Kapitel 2.2 vorgestellten Anforderungen aus Regulatorik und Aufsicht. Ein ineffizientes Monitoring von Zugängen, Zuständigkeiten und genutzten Funktionalitäten führt bei Multicloud-Einsatz zwangsläufig zu (in-)direkten Kosten und der Entstehung einer Schatten-IT durch eine unsachgemäße Anwendung von Cloud-Funktionalitäten durch ungeschultes Personal.

Compliance in Multicloud-Umgebungen ist zusätzlich herausfordernd

Eine zu erwartende anhaltende Diversifizierung der Cloud-Lösungen für die verschiedenen IT-Anwendungsbereiche erfordert mindestens den Aufbau einer Multi-Provider-Steuerung für ein Monitoring von Zuverlässigkeit, Leistung, Sicherheit sowie Kosten, einen Fokus des Managements auf die fachliche sowie technische Konzeption von Schnittstellen zwischen den verschiedenen Providern und die Integration bestehender und neuer SaaS-Lösungen. Hierbei eigneten sich die Tools der Cloud-Anbieter in der Vergangenheit leider meist nur für ein Monitoring der jeweils eigenen Cloud-Produkte.

[39] (interxion, 2019)

4 Compliance as a Service – CaaS

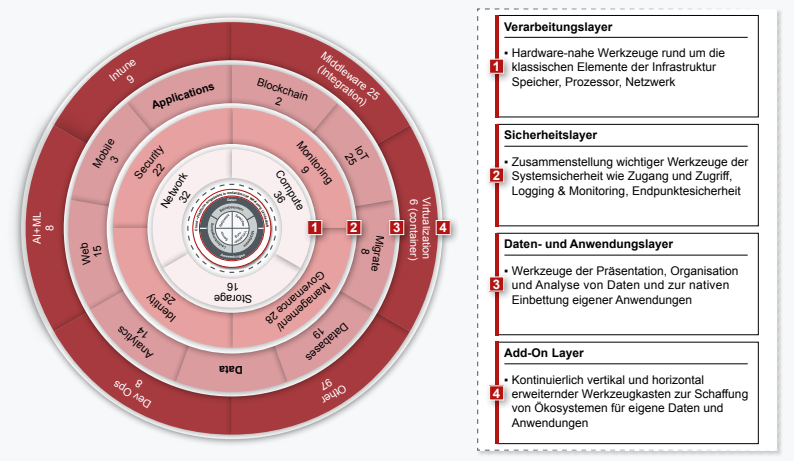
CaaS als Cloud-Baustein erhöht den Reifegrad im Ökosystem

Compliance steht für die Gesamtheit aller Maßnahmen zur Einhaltung äußerer und selbst vorgegebener Regeln. Der Dualismus des Begriffs – einerseits Bezeichnung für die Funktion und Abteilung, andererseits Konzept aller betrieblichen Maßnahmen zur Sicherstellung des rechtmäßigen Verhaltens aller Adressaten in einer Organisation – beinhaltet somit den Weg und das Ziel gleichzeitig. Konkret beschreibt Compliance die Einhaltung selbst vorgegebener (interne Policies) wie von außen aufgegebener Regelungen (Gesetze und Aufsichtspraktiken), dabei dienen viele Policies gerade der Umsetzung der externen Regelungen. Übliche Compliance-Felder fokussieren auf Cybersicherheit, Informationssicherheit und Datenschutz, weitere wesentliche Ziele betreffen zum Beispiel Geldwäsche-Prävention und Vermeidung von Terrorismusfinanzierung.

Cloud-Anbieter haben ein Interesse daran, dem Cloud-Nutzer eine möglichst regelkonforme Cloud-Infrastruktur anbieten zu können. Je mehr Compliance ein Nutzer aus der Cloud beziehen kann, desto leichter kann er das eigentliche Infrastruktur-Angebot nutzen und desto weniger muss er sich selbst um die Compliance-Anforderungen kümmern. Somit kann er auch eine fehlende Expertise in die Cloud externalisieren. Dabei erhalten die Nutzer eine an Best Practices orientierte Compliance-Unterstützung ihrer eigenen, in der Cloud betriebenen, Infrastruktur und Anwendungen.

Nicht zuletzt bieten die verschiedenen Cloud-Anbieter zunehmend weitere Tools an für Compliance, andere Services wie IoT, DevOps, Analytics oder auch für eine effektive Administration anderer Cloud-Angebote innerhalb der eigenen Cloud – Stichwort Multicloud. Beispielhaft stellt die folgende Abbildung 14 die inkludierten Werkzeuge zur Compliance-Unterstützung bei Azure dar.

Rund um den XaaS-Nukleus stellt Azure ein mächtigen Ökosystems mit über 420 Tools in 22 Themengruppen zur Verfügung



Quelle: COREresearch 2021

Abbildung 14: Ökosystem von Azure platziert 423 Tools in 22 Themengruppen organisiert in vier Layern

Anwender können selbst weder die Qualität des XaaS-Nukleus (siehe Abbildung 5 und Abbildung 16) und der Tools noch deren Vielfalt nachbilden. Bezug von Services aus dem Ökosystem ermöglicht dem Anwender die volle Konzentration auf die eigenen, den Wettbewerb differenzierenden Kernkompetenzen.

In den folgenden Unterkapiteln wird für einige Compliance-Felder aufgezeigt, wie die Cloud-Anbieter es ihren Anwendern erleichtern, Compliance mit externen und internen Vorschriften sicherzustellen. Zusätzlich wird mit dem effektiven Management einer Multicloud-Umgebung ein wichtiges Lösungsmuster der Compliance-Unterstützung vorgestellt.

4.1 Cybersicherheit aus der Cloud

Begriffsklärung
Cybersicherheit und IT-Sicherheit stehen synonym für den Schutz von Netzwerken, Geräten und Daten vor unbefugtem Zugriff und die Praxis der Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten. Alle Maßnahmen wirken auf den „Tenant“ des Anwenders.

Azure setzt den Schutz der Daten eines Anwenders mit mannigfaltigen technischen Maßnahmen um. Die Basisstruktur aller Liefermodelle der Cloud IaaS, PaaS und SaaS besteht aus den neun in Abbildung 5 genannten Komponenten (Network bis Applications).

In der Sicherheitsebene Netzwerk stehen vielfältige Sicherheitsmaßnahmen zur Verfügung wie zum Beispiel Netzwerksegmentierung mit Filterung (allow/deny), Regeln (inbound/outbound), erzwungener Tunnelung (Transportverschlüsselung), Routenvorgaben und der Möglichkeit virtualisierte ‚Appliances‘ (Hardware-Firewalls) einzubinden. Selbstredend stehen weitere mächtige Werkzeuge wie Monitoring des Netzwerkverkehrs (Logging & Monitoring), DNS, Global Traffic Routing (Front Door) und Load Balancing (auf den Ebenen App, Netzwerk und Global) parat.

In Anbetracht der kontinuierlich hohen Ausgaben der Hyperscaler für Sicherheit bei Technik und Personal, von denen jeder einzelne Anwender überproportional profitiert, wird der hohe Schutzstandard der eigenen Daten in der Cloud gegenüber der eigenen Serverhaltung ersichtlich. Konkret am Beispiel Azure: 3.500 Sicherheitsexpertinnen und -experten arbeiten nur am Thema Sicherheit und es wird jährlich nur für Sicherheitsmaßnahmen der Betrag von EUR 1 Mrd. ausgegeben.

Hyperscaler sorgen inhärent für hochsicheren IT-Betrieb – im Eigenbetrieb ist das nicht erreichbar

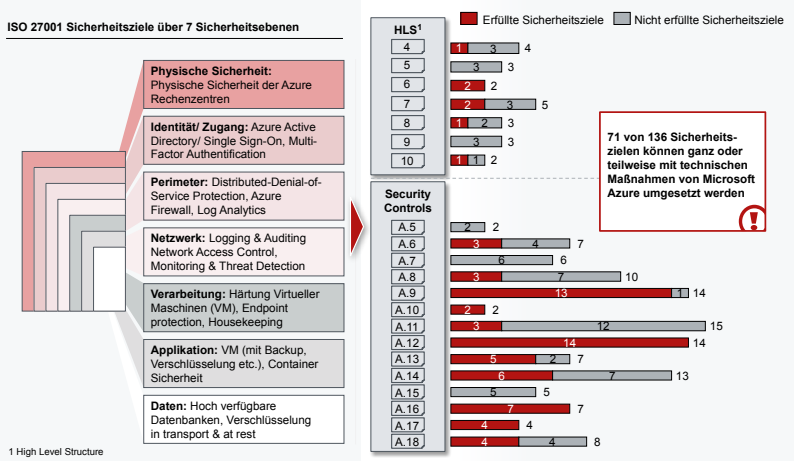
4.2 Informationssicherheit aus der Cloud

Begriffsklärung
Informationssicherheit beinhaltet Cybersicherheit und schützt zudem über Daten hinaus auch Informationen – Daten sind maschinenlesbare Informationen. Die Schutzziele sind für Daten und Informationen gleich: Vertraulichkeit, Integrität und Verfügbarkeit. Informationen können Papierdokumente, das gesprochene Wort in einem Gespräch oder physische Datenträger sein.

Mit Maßnahmen der Informationssicherheit werden nicht nur Informationen, sondern auch Endgeräte gesichert; Beispiele sind die Tools Endpoint Manager – auch MDM: Mobile Device Management – (ermöglicht z.B. remote wipe, das Ausrollen von Unternehmensrichtlinien und Apps und die Überwachung der Compliance-Konformität der Endgeräte) und Defender for Identity Portal (u.a. Überwachung der Nutzeraktivitäten, Schutz der Benutzeridentitäten und Anmeldeinformationen). Diese Maßnahmen wirken über die Maßnahmen der Cybersicherheit hinaus auch auf die eigene Infrastruktur des Nutzers jenseits seines Tenants.

Um den XaaS-Nukleus herum hat Azure ein Ökosystem mit Tools aufgebaut, welche in Abbildung 15 illustriert in ihrer Gesamtheit über sieben Sicherheitsebenen – physische Sicherheit bis zu den Daten – auf die Cybersicherheit des Tenants einzahlen. Von den 136 Themenstellungen des ISO-Standards 27001 (High Level Structure 4 bis 10 und Security Controls A.5 bis A.18) können mit dem Öko-System von Azure 71 ganz oder zumindest teilweise erfüllt werden.

Übersicht ISO 27001 Anforderungen und Anzahl zugehöriger Sicherheitsziele



Quelle: COREresearch 2021

Abbildung 15: Compliance aus der Cloud durch automatisierte technische Prozesse

Clouds erfüllen ca. 50% der Anforderungen aus ISO 27001 „out of the box“

Beispielsweise wird die physische Sicherheit durch die Azure Rechenzentren gewährleistet, welche zutrittsgesichert mit allen baulichen, elektronischen und personellen Maßnahmen geschützt sind. Ausweis dieser Güte der physischen Sicherheit sind passende Zertifikate, welche diese angemessenen Sicherheitsmaßnahmen bestätigen. Diese sind ISO 27001 (TISAX und 27018 beziehen sich wiederum auf 27001 Sicherheitsziel A.11 Physische Sicherheit), BSI C5 stellt eigene Anforderungen an die physische Sicherheit, die im Kapitel „5.5 Physische Sicherheit“ gegliedert sind in die Themen „PS-01 Sicherheitsanforderungen für Räumlichkeiten und Gebäude“, „PS-02 Redundanzmodell“, „PS-03 Perimeterschutz“, „PS-04 Physische Zutrittskontrolle“, „PS-05 Schutz vor Feuer und Rauch“, „PS-06 Schutz vor Ausfall der Versorgungseinrichtungen“ und „PS-07 Überwachung der Betriebs- und Umgebungsparameter“. Auch Sicherheitsanforderungen des US-amerikanischen Verteidigungsministeriums wie DFARS[40] und SRG[41] sind erfüllt.

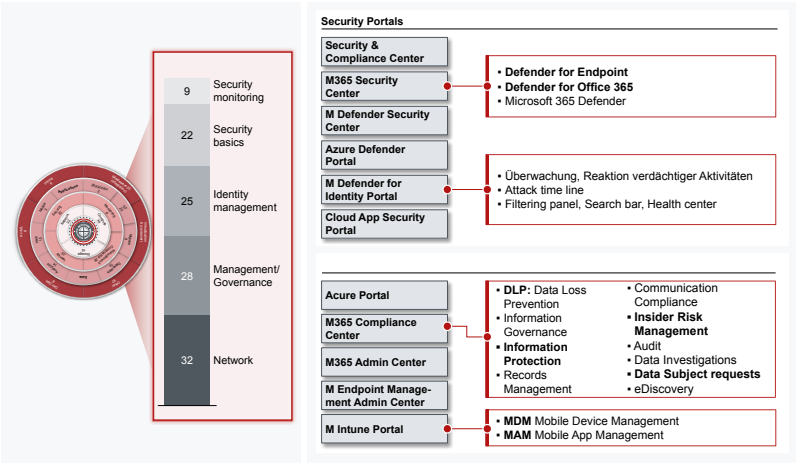
[40] Defense Federal Acquisition Regulation Supplement

[41] Cloud Computing Security Requirements Guide

Business Continuity Management (BCM) ist fester Bestandteil einer Cloud. Zentral für ein BCM sind Backups und ihre funktionssichere Wiedereinspielung (Restore). Hierbei unterstützt Azure auf mehreren Wegen: Einerseits durch automatische Backups aller Speicherinstanzen eines Tenants wie Festplatten, Datenbanken und VMs zugeordneten Speichern. Andererseits wiederum durch die automatisierten Backups einer als SaaS bezogenen Microsoft 365 Instanz. Der Anwender erhält somit aus Azure heraus nicht nur Maßnahmen für seinen eigenen Tenant, sondern auch für seine eigene Unternehmensinfrastruktur jenseits des Tenanten. Um Dinge wie Personal, Governance und alle in Abbildung 15 „nicht erfüllten Sicherheitsziele“ muss er sich weiterhin selbst kümmern.

Abbildung 16 stellt einige Tools im Ökosystem Azure vor. Mit 116 Tools zahlt ca. ein Viertel der Tools direkt auf die Sicherheit ein. Ein Beispiel ist die Informationsklassifizierung von Microsoft 365. Mit Hilfe der bei Microsoft „Information Protection“ genannten Informationsklassifizierung kann der Nutzer seine Office-Dokumente automatisch mit Vertraulichkeitsklassen beschriften (‚Labelling‘) und mit unternehmensweiten Richtlinien (‚Policies‘) je Vertraulichkeitsklasse versehen. Diese Richtlinien entfalten auch ihre Wirkung, wenn der Anwender die klassifizierten Dokumente per E-Mail mit Outlook versenden will. So kann beispielsweise eine E-Mail an einen bestimmten Kunden oder bei Nennung bestimmter Worte automatisch verschlüsselt werden.

Inkludierte Werkzeuge der Cloud-Anbieter (insb. Hyperscaler) tragen wesentlich zur Compliance bei (hier am Beispiel von MS Azure)



Quelle: COREresearch 2021

Abbildung 16: Tools für Compliance und weitere Services am Beispiel Azure

Identitätsmanagement und Informationsklassifizierung verlieren als Compliance-Moniten ihren Schrecken

Für das Identitäts-Management zeichnen 25 Tools verantwortlich. Die Verwaltung von Identitäten und Zugriffen (engl. Identity and Access Management, kurz: IAM) übernimmt in der Microsoft Cloud Azure Active Directory (AAD), das mit dem On-Premise AD von Microsoft synchronisiert werden kann. Mit dem AD werden Nutzerkonten verwaltet. Die komplette Nutzerverwaltung, d.h. On- und Off-Boarding sowie Authentifizierung und Autorisierung, auch von Drittanwendungen, ist über Azure AD organisiert. Das IAM basiert auf der Definition von Rollen und Verantwortlichkeiten im Unternehmen, aus deren Aufgaben sich die dafür notwendigen Tools ableiten lassen. Dies wird in dieser Granularität oft als rollenbasiertes

Zugriffsmanagement (engl. Role Based Access Management, kurz: RBAC) bezeichnet. Die Komplexität der möglichen Zugangs- und Zugriffsberechtigungen ist abhängig von der Anzahl der Rollen, der Tools und der Aktivitäten innerhalb der Tools, mit denen Prinzipien wie Segregation of Duties, Vier-Augen-Prinzip, Least Privilege, Just-in-Time (JIT) Access beim Wartungszugriff auf Produktionsdaten, Multi-Faktor-Authentifizierung (MFA) und ein Passwort Reset im Self Service in die Praxis umgesetzt werden. Des Weiteren bietet Azure AD Schutzfunktionen der verwalteten Identitäten bestehend aus dem Aufzeigen von Schwachstellen und risikobehafteten Konten sowie dem risikobasierten bedingten Zugriff. Zusätzlich steht mit PIM (Privileged Identity Management) die Verwaltung von privilegierten Konten (z. B. Admins) bereit, die bei jeder Aktivierung ein Alerting an ausgewählte Empfänger auslöst. Mit der Automatisierung der Verwaltungstätigkeit wird nicht nur die Fehlerrate reduziert, sondern auch der zeitliche und operative Aufwand. Außerdem werden diese Aktivitäten automatisch protokolliert und sind im Falle einer internen Stichprobe oder eines Audits nachvollziehbar.

Ein weiteres interessantes Werkzeug im IAM-Kasten ist ‚Conditional Access', das verschiedene Signale zusammenführt, um auf deren Basis Entscheidungen zu treffen und Richtlinien durchzusetzen, welche entweder einen Zugriff blockieren, gewähren oder kraft Multi-Faktor-Authentifizierung (MFA) einen zweiten Faktor anfordern. Beispiele sind die vom Aufenthaltsort (Büro/Zuhause, Ausland) abhängige MFA oder ein per KI automatisch errechneter Risikoscore des Logins.

4.3 Datenschutz aus der Cloud

Begriffsklärung
Unter Datenschutz wird der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen („Betroffene") und insbesondere deren Recht auf Schutz personenbezogener Daten verstanden. Datenschutz bedingt eine adäquate Datensicherheit.

Als zentrales Prinzip des Datenschutzes wurde auch die Gewährleistung von Datensicherheit gesetzlich verankert (Art. 5 Abs. 1 lit. f und Art. 32 DSGVO). Datensicherheit ist der Schutz personenbezogener Daten mit geeigneten technischen und organisatorischen Maßnahmen. Die Schutzziele sind Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Wie in den vorherigen Abschnitten gezeigt, trägt Azure in Form von Maßnahmen der IT- und Informationssicherheit als TOM zur Datensicherheit bei.

Cloud-Werkzeuge helfen bei Erfüllung von Betroffenenrechten und Löschpflichten

Darauf aufbauend unterstützt Azure Datenschutz direkt mit den zwei Tools ‚Data Subject Requests' und ‚Records Management'. Die DSGVO regelt in den Artikeln 12 bis 20 die so genannten Betroffenenrechte, d.h. Rechte von Personen, deren personenbezogenen Daten durch Organisationen verarbeitet werden. Dazu gehört das Recht auf transparente Information, ein Auskunftsrecht, ein Recht auf Berichtigung und auf Löschung, das Recht auf Datenübertragbarkeit. Mit dem Tool ‚Data Subject Requests' können Nutzerkonten im Azure AD auf die Anfragen eines Betroffenen hin bearbeitet werden.

Das Tool ‚Records Management' verwaltet u.a. Aufbewahrungs- und Löscheinstellungen für Objekte (Office-Dateien, E-Mails) mit Aufbewahrungszeiträumen und damit Löschfristen. Des Weiteren erlaubt das Tool Einstellungen zu genehmigten (z.B. Lesen erlaubt, Schreiben nicht möglich) und gesperrten (z.B. Löschen nicht möglich) Aktionen vorzunehmen und zusätzlich die Protokollierung aller Aktivitäten zu einem Objekt inkl. Nachweis der vollzogenen Löschung.

4.4 Additive Compliance Tools aus der Cloud

Neben Werkzeugen für IT-Sicherheit, Informationssicherheit und Datenschutz bietet das Öko-System von Azure weitere interessante Tools zur Erfüllung von Compliance-Anforderungen. Die folgenden fünf Compliance-Werkzeuge stellen mächtige Maßnahmenbündel dar und können allgemein die Compliance einer Organisation erhöhen und im speziellen die Themenfelder Geldwäsche-Prävention und Vermeidung von Terrorismusfinanzierung adressieren.

Mit ‚Data Loss Prevention' (DLP) werden E-Mails auf sensible Inhalte untersucht und abhängig vom Ergebnis Aktionen ausgelöst wie eine Rückfrage an den Nutzer, ob er die beabsichtigte Aktion wirklich vornehmen will über die Benachrichtigung einer Kontrollfunktion bis hin zur Untersagung der beabsichtigten Aktion.

Data Loss Prevention ist typisches „dual use" Produkt – nützliches Werkzeug oder schädliche Waffe

Mit ‚Insider Risk Management' werden interne Risiken minimiert, indem böswillige und unbeabsichtigte Aktivitäten in der Organisation erkannt, untersucht und auf diese reagiert wird. Der Anwender kann vorgefertigte Richtlinienvorlagen wählen oder eigene erstellen. Vorlagen gibt es zum Beispiel für Datendiebstahl durch ausscheidende Mitarbeiter, allgemeine Datenlecks, Datenlecks durch privilegierte Rollen (Bsp.: IT-Admin) oder unzufriedene Mitarbeiter.

Mit dem Tool ‚Unified Audit Log' werden die Benutzer- und Admin-Aktivitäten in der Organisation aufgezeichnet. So kann beispielsweise untersucht werden, ob ein Benutzer ein bestimmtes Dokument angesehen oder ein Element aus seiner Mailbox gelöscht hat. Mit dem Tool ‚Data Investigations' kann an allen Microsoft 365 Speicherorten nach sensiblen, bösartigen oder verlegten Daten gesucht werden. Zudem kann untersucht werden, was passiert ist, und Maßnahmen können ergriffen werden. Mit ‚eDiscovery' können Anfragen zur gerichtlichen Offenlegung beantwortet sowie der Benachrichtigungsprozess für Legal Holds verwaltet werden.

4.5 Multicloud-Strategien mit speziellen Fähigkeiten im Provider-Management

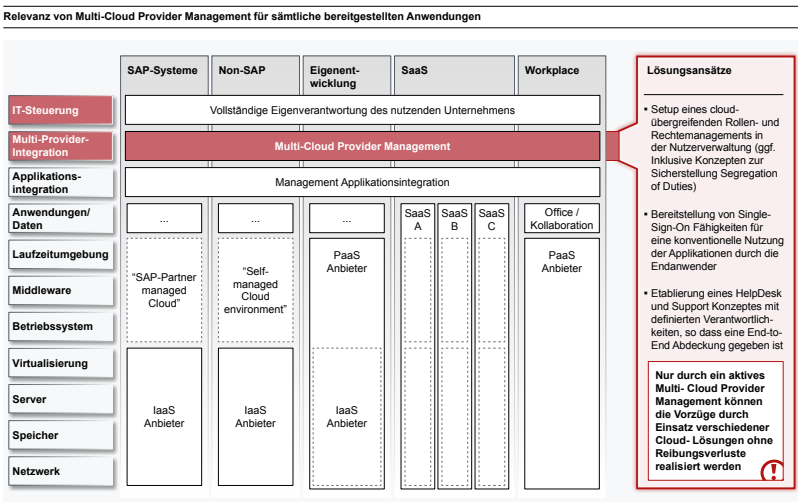
Respektierend, dass Single-Provider-Strategien in Bezug auf Cloud-Nutzung nur in sehr wenigen Unternehmen realistisch umsetzbar sind, müssen die in Kapitel 3.3 dargestellten Herausforderungen adressiert werden. Resultat der strategischen Überlegungen zu den Lösungselementen hierfür sind grundlegende Entscheidungen zur Definition des Zielbildes für die Cloud-Zielarchitektur und das Festlegen von Verantwortlichkeiten.

Multicloud ist für viele Unternehmen eine Notwendigkeit, trotzdem muss das Zielbild explizit und konkret entschieden werden

Invariant zur Entscheidung, ob das Multicloud-Management in Eigenregie oder durch einen Dienstleister betrieben wird, ist sicherzustellen, dass Cloud-Architekten unter Berücksichtigung von Leistungs- und Sicherheitsanforderungen, Lizenzbedingungen und Compliance-Vorgaben ein Portfolio an Cloud-Angeboten zusammenstellen, welches den aktuellen Bedürfnissen des Unternehmens entspricht. Wesentlich hierbei ist es, eine möglichst geringe Komplexität des verfügbaren Marktangebotes einzugehen.

Drei Zielbilder sind möglich:

(1) Ein Zielbild mit einem einzigen Cloud-Anbieter nutzt eine Service-übergreifende Infrastruktur. Hierbei werden alle Anwendungskategorien wie bspw. SAP-Anwendungen, Eigenentwicklungen, Workplace-Anwendungen und Software-as-a-Service Lösungen auf einer IaaS-Plattform aufgebaut. Die Voraussetzung ist, dass eine von allen Anwendungen nutzbare Cloud-Infrastruktur zur Verfügung steht. Häufig steht dieser Option bereits die Unvereinbarkeit der Cloud für bspw. SAP Services mit der Cloud des Workplace-Providers im Wege.
(2) Ausgehend von diesem Idealbild ist die nächstbeste Option eine Aufteilung auf zwei Cloud-Provider. Die Wahl fällt hierbei auf jene Anbieter, welche die Möglichkeiten bieten, sämtliche cloud-basierten Eigenentwicklungen und von Drittanbietern bezogenen Cloud-Anwendungen hierüber abzubilden. Die Auswahl dieser primären Cloud-Provider bestimmt sodann die Grundstruktur der IaaS, in die sich SAP/ non-SAP-Services, Eigenentwicklungen und SaaS-Lösungen integrieren lassen müssen. Konsequenz für nachfolgende Erweiterungen der IT-Infrastruktur ist eine klare Restriktion für sämtliche künftigen Einkaufsentscheidungen und eine vorgegebene Cloud-Technologie für alle weiteren Eigenentwicklungen.
(3) Das komplexeste Zielbild ergibt sich, sollten für das Unternehmen notwendige Anwendungen weder auf die primäre Cloud-Infrastruktur noch auf die ausgewählte Infrastruktur der Workplace-Services migriert werden können. Aufgrund der Herausforderungen einer Integration eines jeden weiteren Cloud-Providers ist es das Ziel, eine Infrastruktur mit drei oder mehr Cloud-Providern nach Möglichkeit zu vermeiden.



Quelle: COREresearch 2021

Abbildung 17: Ausnutzung aller Providerstärken mittels Multi-Cloud Provider Management

Multicloud-Management erfordert spezielle Fähigkeit in der eigenen Organisation

Zwingend erforderlich für die operative Umsetzung einer Multicloud-Strategie sind Kompetenzen im IT-Management, im IT-Service-Management zur operativen Steuerung und Überwachung der Cloud-Dienste, Kapazitäten in der IT-Architektur bzw. IT-Security zur „Inhouse"-Beratung und Gewährleistung einer technischen Sicherheitsarchitektur sowie im IT-Sicherheitsmanagement zur Übernahme operativer Tätigkeiten, insbesondere der Benutzerverwaltung (siehe Abbildung 17).

Unternehmen müssen entscheiden, entweder eigene Ressourcen und Kompetenzen aufzubauen, oder spezialisierte Dienstleister für das Multicloud-Management zu beauftragen. Erste Marktangebote hierfür sind bereits verfügbar, wenn auch der Umfang an echten Erfahrungswerten zunächst gering ist.

Marktangebote für Multicloud-Management entstehen gerade, Erfahrungswerte sind noch gering

Die Angebote der Dienstleister für Multicloud-Management lassen sich in zwei Philosophien klassifizieren. Der Tool-basierte Ansatz versucht die Angebote verschiedener Cloud-Provider auf Basis ihrer Gemeinsamkeiten zu abstrahieren und das Management durch Bereitstellung einer integrierten Benutzeroberfläche zu vereinfachen. Der zweite Ansatz erkennt an, dass durch Abstraktion der Angebote verschiedener Cloud-Provider zwar eine Vereinfachung der Handhabung erzielt wird, gleichzeitig aber die bewusst gewählte Kombination der Stärken verschiedener Provider nicht mehr voll ausgeschöpft wird.

Die Bedürfnisse und Herausforderungen der Kunden bzgl. Multicloud-Management antizipierend, ist davon auszugehen, dass seitens der Anbieter, insbesondere der Hyperscaler, zunehmend integrierende Cloud-Angebote gestaltet werden. So arbeiten Google und Microsoft beispielsweise bereits daran, SAP-Anwendungen auf ihren eigenen Cloud-Infrastrukturen zu betreiben, um Administrationsaufwände und Komplexität ihrer Kunden zu reduzieren. Neben den Hyperscalern bieten auch spezialisierte Anbieter (z. B. meshcloud.io) Bausteine für die wesentlichen Herausforderungen des operativen Betriebs von Multicloud-Umgebungen. Gleichwohl sei an dieser Stelle nochmal unterstrichen, dass es für eine erfolgreiche Umsetzung einer Multicloud-Strategie mehr als die Einführung von Tools bedarf.

5 Fazit

Verzicht auf Cloud-Services bedingt Verzicht auf Exzellenz in eigenen Kernkompetenzen

Cloud ist bereits Commodity. Zumindest die typischen Liefermodelle XaaS à la IaaS, PaaS und SaaS. Wer das noch nicht begriffen hat, der hat nicht nur keine Entschuldigung mehr für den Eigenbetrieb von Hardware, sondern ein zweites Problem: Die Ökosysteme der Hyperscaler können nicht genutzt werden. Diese bringen aber den wahren Mehrwert der Migration in die Cloud. Die Exzellenz der Tools in Qualität und Quantität kann durch Dritte nicht erreicht werden. Und damit kann die Exzellenz der eigenen Kernkompetenz nicht vollumfänglich ihre Wirkung entfalten, wird sie doch jäh durch die Mittelmäßigkeit der eigenverantwortlichen IT ausgebremst.

Es macht keinen Sinn eigene Ressourcen an Geld, Zeit und Expertise in Hardware zu investieren, denn die Digitalisierung macht alles zu Software, und wer Software beherrscht, beherrscht den Markt. Und die Cloud ist die Transformationsmaschine von Hardware zu Software. Sie ist gleichzeitig Fundament, Maschinenraum, Labor und Entwicklungsabteilung der Digitalisierung. Das Fundament bildet der XaaS-Nukleus, das ist das klassische Rechenzentrum eines Unternehmens, somit Server, Festplatten, Appliances, Netzwerke. Bereits damit sind viele Unternehmen, wenn nicht überfordert, dann so stark engagiert, dass weniger Ressourcen für das eigentliche Kerngeschäft zur Verfügung stehen. Dieses Kerngeschäft ist für die allermeisten Unternehmen nicht IT. Der Maschinenraum besteht beispielsweise aus Werkzeugen zur Integration, Virtualisierung, Sicherheit, Governance, IoT und Identitätsmanagement. Das Labor in der Cloud wird aus Tools zum Beispiel für Daten, Analyse, Datenbanken und Blockchain gebildet. Und die Entwicklungsabteilung kann beispielsweise aus Tools für Künstliche Intelligenz (AI), Machine Learning (ML), DevOps, Web Apps und Mobile Apps schöpfen.

Steigende Regulierung zwingt Hyperscaler zu mehr Anstrengungen für Compliance, um ihren Kunden erstens stets eine gesetzeskonforme und zweitens eine das Kerngeschäft der Kunden nicht weiter „störende“ Plattform zu liefern – nicht störend in dem Sinne, dass im besten Falle die Kunden sich nicht mehr um Compliance ihres auf IT beruhenden Geschäfts kümmern müssen. Hierfür stehen mittlerweile auch Tools zur Verfügung, in unterschiedlicher Anzahl und Abdeckung aus regulatorischen Anforderungen zu den Themenkomplexen Geldwäsche-Prävention, Vermeidung von Terrorismusfinanzierung, Datenschutz und Informationssicherheit inkl. IT-Sicherheit. Zu den beiden letztgenannten stehen ungleich mehr Maßnahmen zur Verfügung als zu den ersteren Themenstellungen. Bei der Informationssicherheit kann zum Beispiel eine Cloud-Plattform wie Azure bis zu 71 von 136 Sicherheitszielen des ISO 27001-Standards ganz oder teilweise mit technischen Maßnahmen umsetzen. Das bedeutet konkret, dass ein Cloud-Anwender in diesem Beispiel weniger als die Hälfte dieses Prüfkatalogs mit eigenen Mitteln erfüllen muss. Compliance-as-Code wird mehr und mehr zur Wirklichkeit – zumindest für Cloud-Anwender.

„Software eats the world“ ist das nicht mehr ganz neue Mantra der Digitalisierung. Cloud ist die große Transformationsmaschine von Hardware über Software zur Digitalisierung. Insofern demokratisiert die Cloud die Verfügbarkeit an IT-Ressourcen und über das Ökosystem der Cloud-Tools auch die Entwicklungs- und Fertigungstechniken bis hin zur Künstlichen Intelligenz.

In der Cloud liegt nicht die Zukunft, sondern bereits die Gegenwart. Gibt es keine Zukunft ohne Bewusstsein für die Vergangenheit, so gibt es keine Zukunft ohne die Gegenwart in der Cloud.

Literaturverzeichnis

@DKB.de. (24. März 2020). *twitter.com/DKB_de.* Von https://twitter.com/DKB_de/status/1242417794303606785 abgerufen

Amazon Web Services. (24. August 2006). *Announcing Amazon Elastic Compute Cloud (Amazon EC2) – beta.* Abgerufen am 02. Februar 2021 von https://aws.amazon.com/de/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/

Amazon Web Services. (2015). *AWS-Fallstudie: Stripe.* Abgerufen am 17. März 2021 von aws.amazon.com: https://aws.amazon.com/de/solutions/case-studies/stripe/

Amazon Web Services. (2018). *AWS-Fallbeispiel: Home24.* Abgerufen am 17. März 2021 von aws.amazon.com: https://aws.amazon.com/de/solutions/case-studies/home24/

Amtsblatt der Europäischen Union. (6. Juli 2016). *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und Ratess vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.* Abgerufen am 8. April 2021 von EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

Beiersmann, S. (24. Februar 2016). *Spotify zieht in die Google Cloud um.* Abgerufen am 17. März 2021 von zd.net: https://www.zdnet.de/88260948/spotify-zieht-in-die-google-cloud-um/

Bitkom. (2020). DS-GVO und Corona – *Datenschutzherausforderungen für die Wirtschaft.* Abgerufen am 19. 02 2021 von https://www.bitkom.org/sites/default/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf

Bitkom Research, KPMG. (2020). *Cloud Monitor 2020.* Abgerufen am 02. Februar 2021 von https://www.bitkom.org/sites/default/files/2020-06/prasentation_bitkom_kpmg_pk-cloud-monitor.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI). (Oktober 2020). *Cloud Computing Compliance Criteria Catalogue – C5:2020.* Abgerufen am 8. April 2021 von https://www.bsi.bund.de: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Bundesanstalt für Finanzdienstleistungsaufsicht (BAIT). (26. Oktober 2020). *Bankaufsichtliche Anforderungen an die IT.* Abgerufen am 8. April 2021 von Rundschreiben 10/2017 (BA) in der Fassung vom XX.XX.2020: https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2020/dl_kon_13_20_BAIT.pdf?__blob=publicationFile&v=4

Bundesanstalt für Finanzdienstleistungsaufsicht. (14. September 2018). *Bankaufsichtliche Anforderungen an die IT (BAIT).* Abgerufen am 8. April 2021 von Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9

Bundesanstalt für Finanzdienstleistungsaufsicht. (1. Oktober 2019). *Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT).* Abgerufen am 8. April 2021 von Rundschreiben 11/2019 (WA) in der Fassung vom 01.10.2019: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1911_kait_wa.pdf;jsessionid=1AE63BF6AD0868C106685ACF039322D9.2_cid383?__blob=publicationFile&v=3

Bundesanstalt für Finanzdienstleistungsaufsicht. (20. März 2019). *Versicherungsaufsichtliche Anforderungen an die IT (VAIT).* Abgerufen am 8. April 2021 von Rundschreiben 10/2018 (VA): https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va.pdf?__blob=publicationFile&v=5

Bundesministerium des Innern. (17. Juni 2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* Abgerufen am 8. April 2021 von https://www.bmi.bund.de/: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf;jsessionid=9C09997EB074A0C40F94809302B1297A.1_cid295?__blob=publicationFile&v=3

Buski, M., Dymala, M.-A., & Dr Grudzien, W. (Juni 2020). *Das Ende der Karrent - Datenschutz nutzen.* Von CORE.SE - Technmonitor: https://core.se/fileadmin/WhitePapers/20200616_CORE_Whitepaper_Das_Ende_der_Karenz-Datenschutz_nutzen_DE_v1.0.pdf abgerufen

Caumanns, V. (April 2020). *Geheimnisschutz mit ISO-Normen und.* Abgerufen am 18. März 2021 von dialog.dqs.de: https://dialog.dqs.de/acton/attachment/40656/f-bd8bc3d8-a17f-4325-b9f2-88f3dccdd02f/1/-/-/-/-/Geheimnisschutz%20mit%20ISO-Normen%20und%20DS-GVO.pdf

Cloudride LTD. (07. Januar 2021). *CI/CD as a Service: 10 Solutions for Continuous Integration and Delivery in the Cloud.* Abgerufen am 02. Februar 2021 von medium.com: https://medium.com/@cloudride_il/ci-cd-as-a-service-10-solutions-for-continuous-integration-and-delivery-in-the-cloud-c57e1a74562b

Europäische Kommission. (24. September 2020). *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors.* Abgerufen am 8. April 2021 von EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0595&from=DE

Francke, S. (27. August 2020). *Vertrauen der Finanzdienstleister in die Cloud wächst.* Abgerufen am 8. April 2021 von Springer Professional: https://www.springerprofessional.de/en/bank-it/datenschutz/vertrauen-in-die-cloud-unter-finanzdienstleistern-waechst/18316182

Gartner. (23. Juli 2020). *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020.* Abgerufen am 02. Februar 2021 von https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

IDG Research Services. (2020). *Studie Cloud Native 2020.* Deutschland. Abgerufen am 02. Februar 2021 von https://www2.deloitte.com/content/dam/Deloitte/de/Documents/industry-operations/CloudNative_IDG-Studie_Deloitte_2020.pdf

IDG Research Services. (2020). *Studie Cloud-ERP 2021.* Abgerufen am 02. Februar 2021 von https://whitepaper.cio.de/uploads/files/03f246457d0b42b7474bb53bcc0b3ae6eec2dfb0.pdf

interxion. (14. Mai 2019). *Fast alle Unternehmen in Deutschland beschäftigen sich mit der Multi-Cloud.* Abgerufen am 8. April 2021 von interxion.com: https://www.interxion.com/de/whitepapers/cloud-trends--wege-aus-dem-cloud-chaos

ISO (International Organization for Standardization). (Oktober 2013). *Information technology — Security techniques — Information security management systems — Requirements.* Abgerufen am 8. April 2021 von ISO/IEC 27001:2013: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Kirchner, C. (25. März 2020). *Das Online-Brokerage der DKB geht erneut in die Knie.* Abgerufen am 02. Februar 2021 von https://finanz-szene.de/digital-banking/das-online-brokerage-der-dkb-geht-erneut-in-die-knie/: https://finanz-szene.de/digital-banking/das-online-brokerage-der-dkb-geht-erneut-in-die-knie/

Lemos, R. (15. April 2010). *Cloud Computing: Early Adopters Share Five Key Lessons.* (cio.com, Hrsg.) Abgerufen am 17. März 2021 von cio.com: https://www.cio.com/article/2418957/cloud-computing--early-adopters-share-five-key-lessons.html

Lünendonk & Hossenfelder. (2020). *Cloud Transformation – Strategien und Maßnahmen von Banken und Versicherungen auf dem Weg in die Cloud.* Abgerufen am 02. Februar 2021 von https://www.luenendonk.de/produkte/studien-publikationen/luenendonk-trendstudie-2020-cloud-transformation-strategien-und-massnahmen-von-banken-und-versicherungen-auf-dem-weg-in-die-cloud/

Lünendonk & Hossenfelder. (2020). *Digital Outlook 2025: Financial Services.* Abgerufen am 19. 02 2021 von https://www.luenendonk.de/produkte/studien-publikationen/luenendonk-studie-2020-digital-outlook-2025-financial-services/

National Institute of Standards and Technology. (September 2011). *The NIST Definition of Cloud Computing.* (U. D. Commerce, Hrsg.) Abgerufen am 02. Februar 2021 von https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Netflix. (11. Februar 2016). *Completing the Netflix Cloud Migration.* Abgerufen am 17. März 2021 von Netflix.com: https://about.netflix.com/en/news/completing-the-netflix-cloud-migration

Reckwitz, A. (2019). Das Ende der Illusionen. Politik, Ökonomie und Kultur in der Spätmoderne. Berlin: Suhrkamp Verlag.

Verfasser

Nicolas Freitag ist Transformation Manager bei CORE. Seine Erfahrungen aus der Ausbildung zum Bankkaufmann, dem Studium der Wirtschaftswissenschaften und der langjährigen Entwicklung deutschlandweiter Karriere-Netzwerke setzt Nicolas für Klienten bei der Erarbeitung von Unternehmensstrategien, der Entwicklung von digitalen Geschäftsmodellen sowie der Steuerung agiler Software-Entwicklungen ein.

Nicolas Freitag
nicolas.freitag@core.se

Markus Frik ist Transformation Associate bei CORE. Der studierte technische Volkswirt (KIT) konnte Erfahrungen in verschiedenen Cloud-Transformationsprojekten sammeln. Er begleitet Klienten aus der Finanzindustrie zur Implementierung von Anwendungen von der Spezifikation bis zum Go-Live und er baut Managementsysteme für Informationssicherheit und Anti-Financial-Crime auf.

Markus Frik
markus.frik@core.se

Waldemar Grudzien ist Expert Director bei CORE. Er verfügt über 26 Jahre Beratungserfahrung und ist vertraut mit den besonderen Herausforderungen von Compliance getriebenen IT-Transformationen. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientenstrukturen.

Dr. Waldemar Grudzien
waldemar.grudzien@core.se

Nadine Hofmann ist Expert Manager bei CORE. Sie studierte Luft- und Raumfahrttechnik in Braunschweig und Dresden. Ihre Beratungskompetenz fokussiert sich auf technischen Datenschutz und Informationssicherheit (Schwerpunkte IAM, Management von Risiken, ISO27001 und DSGVO). Sie unterstützt Klienten bei der Strukturierung und dem Aufbau von Financial Compliance Systemen.

Nadine Hofmann
nadine.hofmann@core.se

Autorenteam

Christian Böhning ist Managing Director bei CORE. Er besitzt langjährige Erfahrung in der Durchführung digitaler Transformationsvorhaben in durch IT nachhaltig veränderten Branchen. Schwerpunkt seiner Arbeit sind Programme zur IT-Architekturmodernisierung, Durchführung von Compliance-Initiativen und Neuausrichtung von IT-Organisationen.

Christian Böhning
christian.boehning@core.se

Philipp Gampe ist Engineering Manager bei CORE. Er studierte Informatik in Bonn und Potsdam. Als Spezialist für Cloud-Infrastrukturen und Architekturen setzt er neue Projekte in der Cloud um und hilft bei der Migration bestehender Anwendungen. Darüber hinaus unterstützt er bei der Automatisierung der Deployment- und Entwicklungsprozesse sowie dem umfassenden automatisierten Testen.

Philipp Gampe
philipp.gampe@core.se

Calvin Klee ist Transformation Manager bei CORE. Er absolvierte seinen Bachelor of Science in Management an der Royal Holloway University of London. Calvin verfügt über Erfahrungen in der Migration von Kernbankensystemen und Implementierung von Zahlungsverkehrsplattformen. Schwerpunkt seiner Tätigkeit bildet die Koordinierung des Projektmanagements sowie der Orchestrierung von Business Cases.

Calvin Klee
calvin.klee@core.se

Ronny Raschkowan ist Expert Manager bei CORE. Er studierte BWL und Internationale Beziehungen. Ronny leitet die IT-Abteilung bei CORE und unterstützt Kunden bei Cloud-Migrationen mit Schwerpunkt auf Infrastrukturen, Modern Workplace und Mobile Device Management. Seine Erfahrungen zu ISO-27001 Zertifizierung und als Stellv. ISB bei CORE runden seine Security-Experise ab.

Ronny Raschkowan
ronny.raschkowan@core.se

Über COREresearch

Als unabhängiger Technologie Think Tank erforschen wir die Systematik technologisch getriebener Transformationen in Industrien mit einem hohen Anteil an IT im Wertschöpfungsprozess. Im Rahmen unserer Forschungsaktivitäten analysieren wir Märkte und Technologien, thematisieren Strukturen, Ursachen und Wirkmechanismen des technologischen Wandels und kuratieren Ergebnisse für Klienten und die Öffentlichkeit. Darüber hinaus stellen wir ausgewählte Resultate unserer interdisziplinären Forschungen im Rahmen von übergreifenden Publikationen, Einzelstudien sowie Vorträgen einer breiteren Öffentlichkeit zur Verfügung.

CORE

https://core.se

https://core.se/publications/white-papers

Disclaimer

CORE SE
Am Sandwerder 21–23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21–23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se