AWK Group
Enabling digital performance.

AWK FOKUS

Cloud-Einsatz im regulierten Umfeld

In dieser Ausgabe

Die Reise in die Cloud im regulierten Umfeld

«Als Enabler der Digitalisierung ist die Cloud auch im regulierten Umfeld zentral und für moderne IT-Lösungen unerlässlich.»

Christian Mauz
Partner

Es stellt sich nicht mehr die Frage, ob die Cloud kommt oder nicht. Die Entscheidung ist längst gefallen. Die Cloud-Anbieter haben ihre Hausaufgaben gemacht und die Grundlagen für eine sichere Nutzung von Cloud-Diensten geschaffen. Allerdings gibt es speziell im regulierten Umfeld verschiedene Rahmenbedingungen, die für eine konforme Umsetzung von Cloud-Strategien zwingend zu berücksichtigen sind.
Christian Mauz

Die Cloud ist als zentraler Wegbereiter der digitalen Transformation auch im regulierten Umfeld breit anerkannt. Doch die mit der Cloud-Nutzung verbundenen Herausforderungen sind vielfältig. Was muss in der Cloud-Strategie berücksichtigt werden? Wie ist die Governance zu gestalten? Welche Rollen, Prozesse und Richtlinien braucht es für eine sichere und konforme Cloud-Nutzung? Wie ist die Cloud-Migration von Anwendungen anzugehen, die bislang vor Ort betrieben werden – und: Was bedeutet dies für meine Organisation und mein Betriebsmodell? Die gute Nachricht: Viele Hürden sind von den Vorreitern bereits erfolgreich überwunden worden. Das Rad muss also nicht neu erfunden werden. Auch die Unterstützung der Cloud-Anbieter ist insbesondere aufseiten der Hyperscaler vorhanden. Trotzdem haben die IT-Organisationen mit der Cloud-Transformation eine Herkulesaufgabe vor sich. Mit unserem aktuellen Fokus möchten wir Ihnen auf Ihre Reise in die Cloud ein paar Denkanstösse mitgeben.

Spannend in diesem Kontext ist auch die grosse europäische Cloud-Initiative GAIA-X, die darauf abzielt, nach wie vor bestehende Vorbehalte gegenüber der Cloud abzubauen. Gestartet wurde GAIA-X von Vertretern aus Wirtschaft, Wissenschaft und Verwaltung aus Deutschland und Frankreich mit dem Ziel, gemeinsam mit weiteren europäischen Partnern Standards und Regeln für eine Next-Generation-Dateninfrastruktur zu entwickeln. GAIA-X repräsentiert ein offenes, transparentes und sicheres digitales Ökosystem, in dem Daten und Dienste in einem vertrauenswürdigen Umfeld gesammelt, zur Verfügung gestellt und gemeinsam genutzt werden können. Ein zentrales Element dabei ist die Stärkung der digitalen Souveränität und der Datensouveränität, um den Nutzern die vollständige Kontrolle über gespeicherte und verarbeitete Daten zu garantieren.

Wir wünschen Ihnen eine spannende Lektüre.

Cloud im regulierten Bereich – eine anspruchsvolle Transformation

Im regulierten Umfeld bestehen neben den für alle Organisationen geltenden rechtlichen Rahmenbedingungen des Gesetzgebers zusätzliche, weitergehende oder verschärfte Normen und Handlungsanweisungen von Regulatoren. Diese betreffen zunehmend auch die digitalen Geschäftsprozesse und definieren die kommerziellen und technischen Rahmenbedingungen zur Integration und Nutzung von Cloud-Services. Die Cloud-Transformation geht daher mit Veränderungsbedarf bei der Governance einher und erfordert eine bewusste Anpassung der Kultur.

Adrian Anderegg, Marc Raum, Thomas Vogt, Tom Schons

Zu den wichtigsten Treibern für die zunehmende Nutzung von Cloud-Services – nicht nur im regulierten Umfeld – gehören:

- Virtuelle Zusammenarbeit innerhalb der Organisationen sowie mit externen Partnern, insbesondere bei den Kommunikations- und Kollaborationsprozessen

- Rasche und automatisierte Bereitstellung von Umgebungen
- «Capacity on Demand», um Lastspitzen flexibel abzufedern und nur die Nutzung zu bezahlen
- Massgebliche, nicht funktionale Eigenschaften, wie z. B. feingranulare Sicherheitsfunktionen, sowie Cyber-Security- und Privacy-Fähigkeiten
- Rasche Weiterentwicklung und Verfügbarkeit moderner Technologie-Lösungsblöcke
- Anbieter stellen neue Lösungen nur noch als Cloud-Services zur Verfügung
- Fokussierung der eigenen Kompetenzen auf eine höhere Ebene der IT-Wertschöpfung

Was sind die Herausforderungen, Hindernisse und Risiken?

Der Bund hat in seinem Bericht zur «Bedarfsabklärung für eine «Swiss Cloud[1]» die unklaren Rahmenbedingungen zur Nutzung von Public Cloud Services als grosses Hindernis identifiziert. Während die Finanzindustrie entsprechende Leitfäden und Richtlinien für die Cloud-Nutzung bereits erarbeitet hat, wird der Einsatz von Cloud-Diensten im öffentlichen Sektor oft durch Datenschutzgesetze sowie den Straftatbestand der Amtsgeheimnisverletzung (Art. 320 StGB) verhindert.

[1] https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

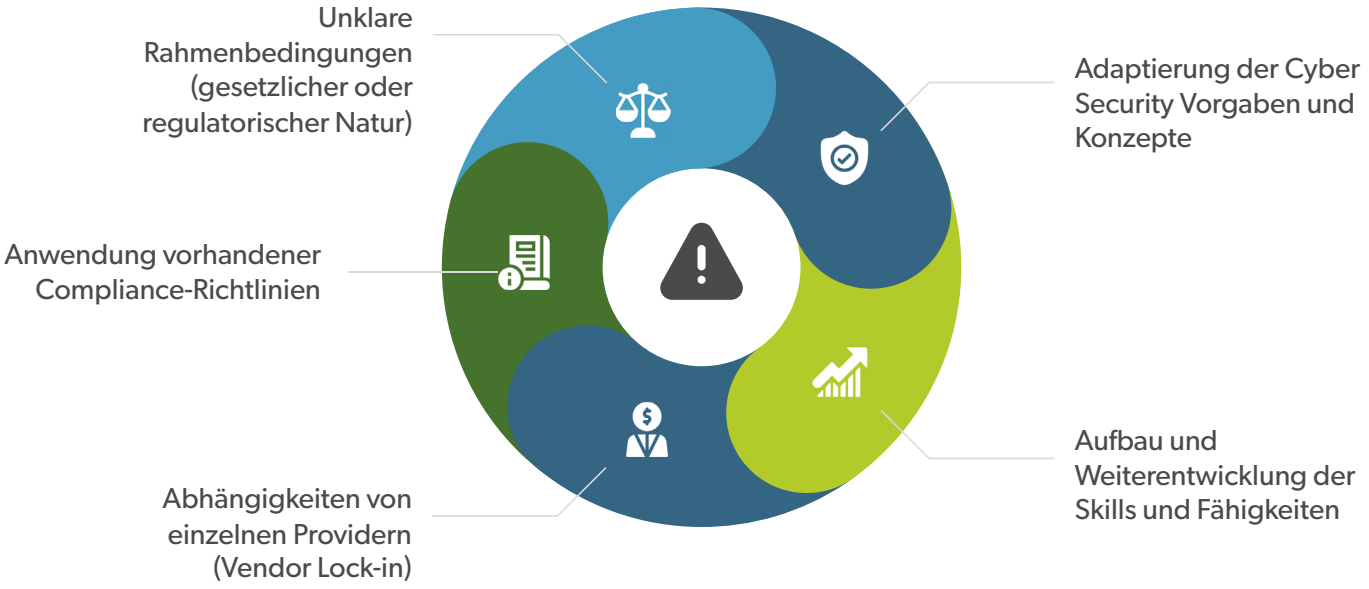


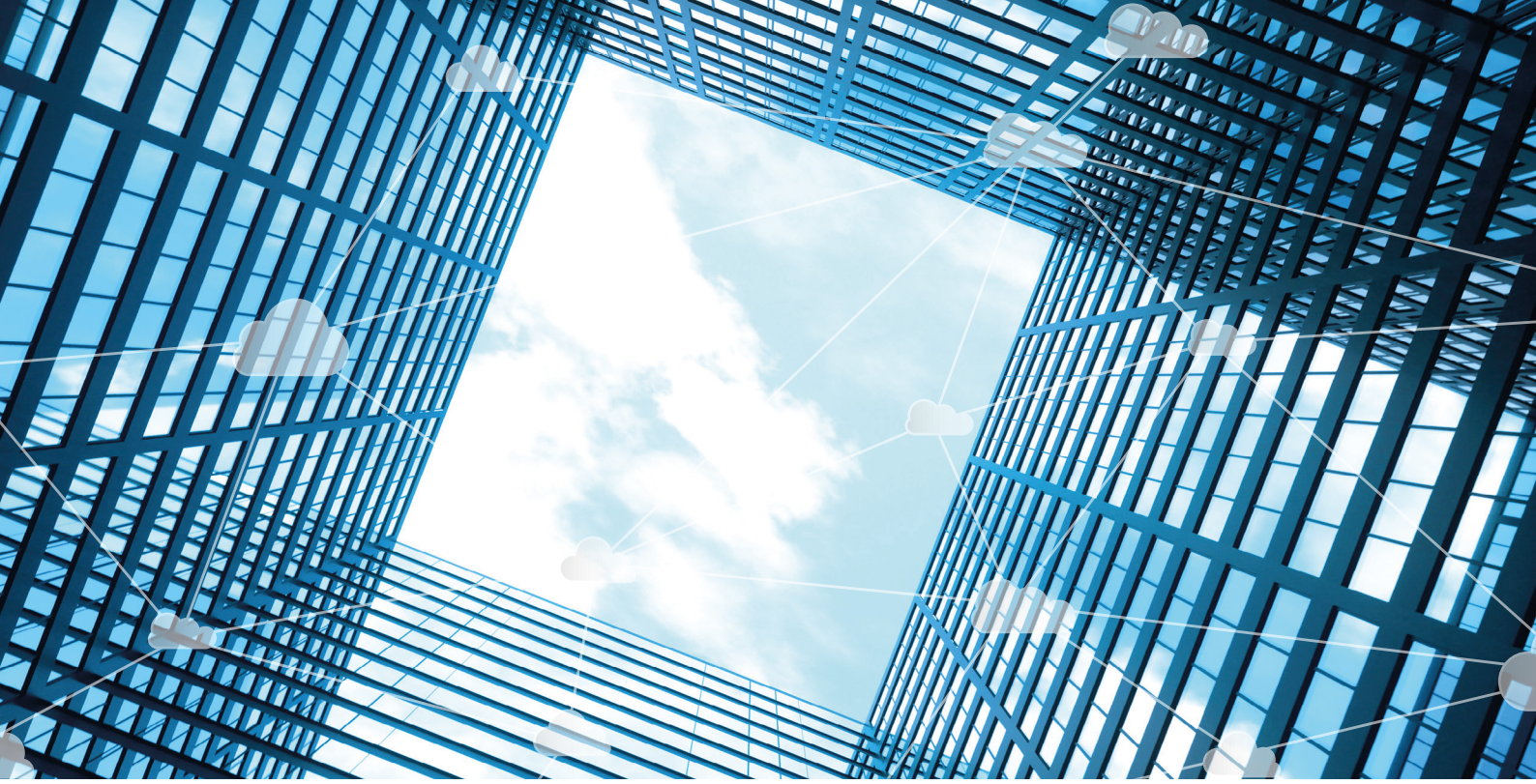
Abbildung 1: Kritische Hindernisse für die Nutzung der Cloud

Vorhandene Compliance-Richtlinien müssen angepasst werden, beispielsweise bei der vertraglichen Verankerung des Audit-Rechts bei Sourcing-Verträgen, da dies im Public-Cloud-Umfeld oft nur durch die Einhaltung einschlägiger Zertifizierungen umsetzbar ist. Cyber-Security-Vorgaben und -Konzepte wie das Netzwerk-Zonenkonzept oder die Integration vorhandener SIEM[2]-Prozesse für Anwendungen in der Cloud müssen neu bewertet und konzipiert werden. Auch die Verfügbarkeit von Cloud-Spezialisten ist aufgrund des «War for Talents» eine Herausforderung. Darüber hinaus gilt es, dem Risiko des Vendor Lock-in, also der langfristigen Abhängigkeit von einem einzelnen Provider, Rechnung zu tragen. In der Praxis zeigt sich, dass es viel Wissen und Disziplin braucht, um auf der technischen Ebene Entscheidungen zu treffen, die wirtschaftlich nachhaltige Wechselmöglichkeiten aufrechterhalten.

Empfohlene Elemente einer Cloud-Strategie

Eine Cloud-Strategie beinhaltet eine klare **Vision und Mission** sowie ein **Zielbild** für die Cloud-Transformation, das insbesondere die organisatorischen Aspekte bezüglich der Einbettung in die digitale Transformation der gesamten Organisation adressiert. Von zentraler Bedeutung sind **Grundsätze zur Cloud-Nutzung** als richtungsweisende Entscheidungsgrundlagen. Des Weiteren müssen die **Risiken der Cloud-Nutzung** analysiert und bewertet werden, unter Einbezug der Branchenempfehlungen (z. B. Cloud-Leitfaden der Schweizerischen Bankiervereinigung). Selbstverständlich ist auch eine **wirtschaftliche Betrachtung der Cloud-Nutzung** wichtig, um eine belastbare Grundlage für die zu erwartenden Veränderungen aus Sicht der gesamten IT-Organisation zu schaffen. Weitere wesentliche Aspekte sind die Definition der zukünftigen **Governance** sowie des **angestrebten Betriebsmodells,** inklusive der übergreifenden organisatorischen Rahmenbedingungen, der Bereitstellung der nötigen Fähigkeiten und allfälliger Sourcingmodelle. Darauf aufbauend müssen die groben Vorgehensschritte und die zu involvierenden Stellen und Entscheidungsgremien zur **Evaluation und Beschaffung der Cloud-Services** geregelt werden. Zudem sind die **Massnahmen** für das **Business Continuity Management (BCM)** sowie die **Leitlinien** für eine **mögliche Exit-Strategie** aus der Cloud heraus festzulegen. Letztendlich gilt es, die umzusetzenden Initiativen der Cloud-Transformation im Rahmen einer mehrjährigen **Roadmap** zu definieren. Dies fordert das Führungsteam, da bestehende Prinzipien, Arbeitsweisen und die Organisation angepasst werden müssen.

[2] SIEM: Security Information and Event Management



Die Umsetzung der Cloud-Strategie

Wir empfehlen, die Operationalisierung und Verankerung der definierten Cloud-Strategie auf mehrere Phasen mit unterschiedlichen Schwerpunkten aufzuteilen, die integral geplant und umgesetzt werden. Basis dafür sind die Cloud-Governance, welche die organisatorischen Rahmenbedingungen adressiert, sowie die übergreifende Cloud-Architektur. Letztere sollte die bestehende Enterprise-Architektur und die technologischen Abhängigkeiten zu bestehenden Lösungsbausteinen berücksichtigen.

Besonderes Augenmerk sollte auf der Anpassung der vorhanden ICT-Sicherheitsarchitekturen liegen. Für die konkrete Cloud-Migration von Anwendungen lohnt sich ein vorgängiges Cloud Readiness Assessment zur Bestimmung des optimalen Zielzustands der Anwendung und des effektiven Migrationsvorgehens. Um Risiken einzugrenzen und Erfahrungen zu sammeln, bietet sich für die einzelnen Cloud-Migrationsvorhaben in den meisten Fällen ein agiles beziehungsweise iteratives Vorgehen an.

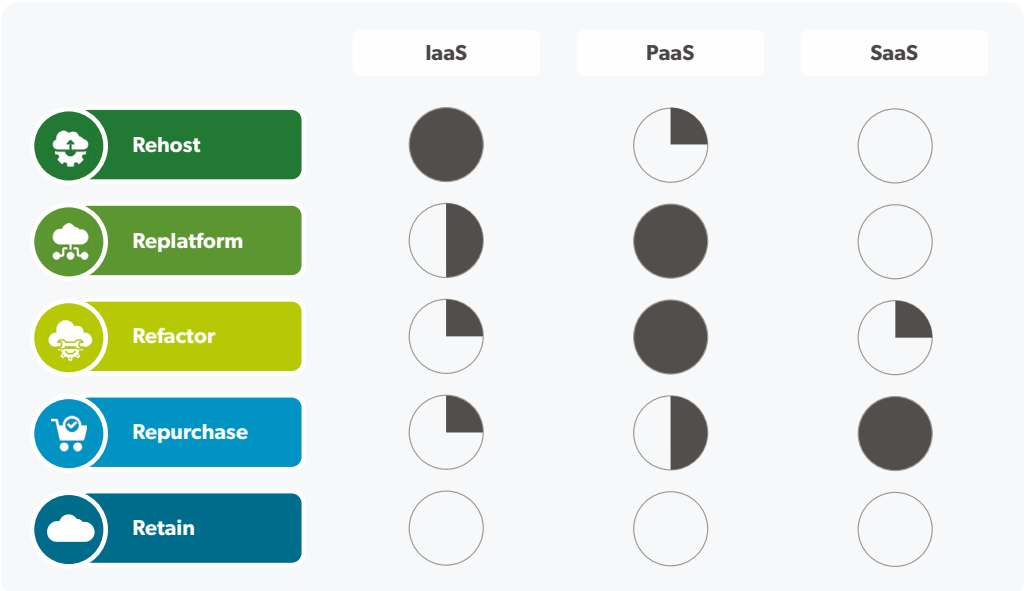


Abbildung 2: Standardstrategien für die Migration von Anwendungen

Abbildung 3:
Die Umsetzung der Cloud-Strategie

Die Public Cloud Provider und das regulierte Umfeld

Die Public Cloud Provider bieten in vielen Bereichen bereits sehr gute Rahmenbedingungen für das regulierte Umfeld an. Oft ist der geografische beziehungsweise rechtliche Standort der Datenspeicherung und -verarbeitung entscheidend. Dieser Aspekt wird durch bereits verfügbare oder angekündigte RZ-Standorte der Public Cloud Provider in der Schweiz adressiert. Zusätzlich bieten diese Provider eine breite Auswahl an regulations- und industriespezifischen Zertifizierungsnachweisen an.

Attraktiv sind die extrem hohen Verfügbarkeiten sowie die mannigfaltigen Möglichkeiten für redundante Konfigurationen der Services auf den Plattformen der Hyperscaler. Denn höhere Service Levels bedingen keine höheren und fixen Investitionen, da sie sich nur in den Servicekosten niederschlagen.

Die heutigen Cloud-Plattformen stellen zunehmend branchenspezifische Cloud-Services zur Verfügung, beispielsweise in Form von Konfigurations-Blueprints zur Erfüllung von Compliance-Anforderungen. Zudem können bestehende Cyber-Security-Konzepte im Rahmen der Cloud-Transformationen substanziell weiterentwickelt und in Bezug auf ihre Wirksamkeit optimiert werden.

Fazit: Cloud-Services sind im regulierten Umfeld nicht mehr wegzudenken.

Damit sich die damit verbundenen Erwartungen erfüllen, ist es jedoch wichtig, die strategischen Entscheidungen sowie die Konzeption und Umsetzung einer Cloud-Transformation im jeweiligen Kontext ausführlich zu betrachten und die Rahmenbedingungen der jeweiligen Organisation zu berücksichtigen.

Das Fundament bildet die Cloud-Strategie, die mit einem klaren Zielbild die strategischen Grundlagen schafft. Potenzielle Risiken sind frühzeitig zu adressieren. Zugleich gilt es, klare Leitlinien zu den wirtschaftlichen und organisatorischen Aspekten der Cloud-Nutzung zu definieren.

In der zweiten Phase sind die Cloud-Governance und die Cloud-Zielarchitektur zu definieren. Die Migration in die Cloud erfolgt mit Vorteil iterativ, um die erforderlichen Fähigkeiten sukzessive aufzubauen und die Risiken zu beherrschen. Durch die rasante Weiterentwicklung der Cloud-Services und -Modelle müssen die definierten Rahmenbedingungen für die Cloud-Nutzung regelmässig geprüft und weiterentwickelt werden.

Die AWK Group unterstützt Organisationen im regulierten Umfeld gerne mit ihrer Expertise und Erfahrung, sowohl bei der Erarbeitung von Cloud-Strategien und entsprechenden Konzeptionen wie auch bei der Umsetzung von Cloud-Transformationen.

Inwiefern kann GAIA-X relevant werden?

GAIA-X[3] ist ein europäisches Projekt zum Aufbau einer Dateninfrastruktur für Europa, die nicht nur leistungs- und wettbewerbsfähig, sondern auch sicher und vertrauenswürdig ist. Zurzeit wird das Projekt insbesondere von Vertretern aus Wirtschaft, Wissenschaft und Verwaltung aus Deutschland und Frankreich getragen, steht aber auch weiteren Partnern offen, die daran teilnehmen möchten. Daher ist es auch für die Schweiz ein interessantes Vorhaben eines politischen Partners mit weitgehend deckungsgleichen Rechtsvorstellungen (z. B. EU-DSGVO).

Das Konzept von GAIA-X basiert auf der obersten Architekturebene auf den Elementen «Föderierte Dienste», «Datenräume» und «Services, die über gemeinsam festgelegte Standards interoperabel sind. Jede teilnehmende Instanz kann GAIA-X-basierende Services anbieten und konsumieren. Über die Standardisierung sind dabei sowohl die technologischen Grundlagen klar definiert als auch die einzuhaltenden Güteklassen (Qualitätskriterien der Services) einheitlich implementiert. Über dieses Konzept wird bei der Nutzung von Cloud Services im Wesentlichen die Abhängigkeit von einzelnen Anbietern beziehungsweise Cloud-Providern mitigiert.

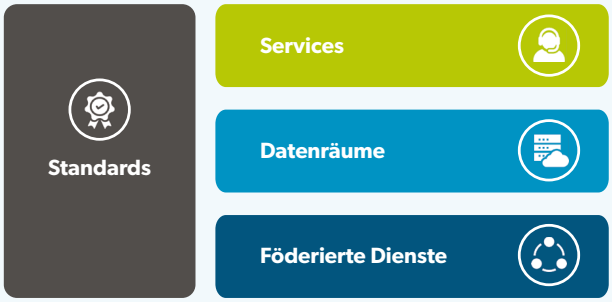


Abbildung 4: Das Konzept von GAIA-X

Selbst wenn GAIA-X heute noch wenig konkret Nutzbares anbietet, könnte die Initiative mit diesen Ansätzen mittelfristig für regulierte Organisationen einen wichtigen Beitrag leisten. Entsprechend lohnt es sich, die Entwicklungen hier genau weiterzuverfolgen und eine Partizipation zu prüfen.

[3] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Erfüllung hoher Cyber-Security-Standards in der Cloud

Die Cloud bietet Unternehmen die Chance, ihre Cyber Security Standards zu erhöhen und bei der Migration konsequent von Anfang an umzusetzen. Besonders für KMU dürfte der Wechsel in eine Cloud-Umgebung mit deutlichen Sicherheitsgewinnen gegenüber ihrer bestehenden On-Premise-Infrastruktur einhergehen, da sie von standardisierten Security Features und dem technischen Fortschritt der Provider gegenüber grossen Unternehmen überproportional profitieren.

Unabhängig von der Unternehmensgrösse gilt es zur sicheren Ausgestaltung und Nutzung von Cloud-Lösungen allerdings, einige zentrale Punkte zu beachten. Vorgängig zur Migration in die Cloud sollte eine detaillierte (Cyber-)Risikoanalyse vorgenommen werden, die alle relevanten Stakeholder innerhalb des Unternehmens involviert. Dem Risikoappetit entsprechende, mitigierende Massnahmen können damit frühzeitig definiert, in entsprechende (Sicherheits-) Konzepte einfliessen und anschliessend umgesetzt werden. Selbstverständlich darf dabei eine kontinuierliche weitere Beobachtung der identifizierten Risiken nicht ignoriert werden.

Zu den grössten Schwierigkeiten aus Security-Sicht gehört die Nutzung von hybriden Cloud-Modellen, die sich in den kommenden Jahren als Normalzustand etablieren wird. Nur wenige Unternehmen werden vollumfänglich in eine einzelne Cloud migrieren. Die meisten werden einen Teil ihrer Anwendungen weiterhin vor Ort betreiben oder sogar in verschiedene Clouds migrieren. Die Sicherheit der Gesamtlösung ist daher elementar mit den (Sicherheits-)Architekturkonzepten und deren Umsetzung verbunden. Das «Shared Responsibility Model», das Anbieter und Nutzer von Cloud-Lösungen zur klaren Abgrenzung der Verantwortlichkeiten zwingt, verursacht jedoch bei Cloud-Neulingen oftmals Konfusion, gefolgt von einer unklaren Auslegung der Verantwortlichkeiten und damit letztlich von (unbewussten) Sicherheitslücken. Zusätzlich werden insbesondere das Identity & Access Management (IAM) sowie die Integration diverser Cloud-Identitäten und deren Berechtigungsverwaltung, zunehmend komplexer und setzen dediziertes Know-how voraus. IAM und Security-Architektur werden damit zu einem zentralen Baustein in der Absicherung von Cloud-Lösungen. Abschliessend müssen auch klassische Security-Aspekte detailliert betrachtet werden, beispielsweise das Security Event Monitoring und die Threat Detection, welche durch die dezentralen Strukturen hybrider Cloud-Modelle vor ganz neue Herausforderungen gestellt werden. Umso wichtiger ist es, Fragestellungen wie: «Wo werden welche Logs kurzfristig / dauerhaft gespeichert? Wie stelle ich sicher, dass mein SIEM ein holistisches Gesamtbild hat? Wie schütze ich die Vielzahl von (API-)Schnittstellen möglichst effizient?», sollten deshalb bereits im Vorfeld klar beantwortet sein.

Es empfiehlt sich daher, grundsätzlich auf etablierte Standards, Vorgehensweisen und Best Practices zu setzen, wie beispielswiese diejenigen der Cloud Security Alliance (CSA).

Cloud in der Finanzindustrie – in mancher Hinsicht eine Herausforderung

In der Finanzindustrie gelten strenge regulatorische, Compliance- und Risikovorgaben für die Umsetzung technischer und organisatorischer Vorhaben. Aufgrund des Schweizer Bankgeheimnisses wurde bis dato zumeist an einem Datenstandort innerhalb der Schweiz festgehalten, während ein Outsourcing ins Ausland als nicht durchführbar galt. Mangels Verfügbarkeit von Public-Cloud-Anbietern auf Schweizer Boden verblieb einzig die Option eines klassischen Hostings mit Schweizer Anbietern. Der Aufbau von Cloud-Rechenzentren in der Schweiz hat diesen Trend jedoch durchbrochen und den Markt zu Gunsten von ausländischen Public-Cloud-Anbietern verändert. Dies insbesondere aufgrund der Zusage der Anbieter, auf eine Datenhaltung in der Schweiz zu setzen.

Adrian Anderegg, Tom Schons

Als federführende Aufsichtsbehörde hat die FINMA bereits 2017 das Rundschreiben «2018/3 Outsourcing» veröffentlicht und dieses im Winter 2020 überarbeitet. Das Rundschreiben regelt nicht nur das angemessene Rahmenwerk für ein klassisches Outsourcing zu IT-Dienstleistern, sondern hat auch entscheidende Auswirkungen auf die Nutzung von Public Clouds. Da die korrekte Auslegung einzelner Paragrafen in Bezug auf Cloud Computing vielfach nicht trivial ist, hat die Schweizerische Bankiervereinigung im Sommer 2020 einen «Cloud-Leitfaden» mit Best Practices veröffentlicht. Doch dem Leitfaden fehlt es nicht nur an Konkretisierungen in Bezug auf einzelne Cloud-Lösungen, sondern auch an technischen und organisatorischen Handlungs- und Umsetzungsempfehlungen. Die bestehenden Lücken müssen die Institute und ihre Dienstleister in eigener Regie schliessen.

Zentrale Aspekte und Stolpersteine in der Umsetzung von Public Cloud Lösungen

Die Auslegeordnung, welche Funktionen und Daten ein Institut in die Cloud verlagert, hat signifikante Auswirkungen auf die Anwendbarkeit des «wesentlichen» oder «nicht wesentlichen» Outsourcings. Die korrekte Triage gemäss Rundschreiben 2018/3 ist an dieser Stelle elementar. Risikobehaftet ist in der Praxis primär die Auslegung als «nicht wesentliches Outsourcing», das durch den kontinuierlichen Ausbau von Cloud-Lösungen mit der Zeit zu einem «wesentlichen Outsourcing» mutiert. Institute, die ihre Cloud-Vorhaben zunächst parkieren, sollten besonderes Augenmerk auf das erhöhte Risiko einer «Schatten-IT» legen, die beispielsweise durch die vergleichsweise einfache Bereitstellung und Nutzung von SaaS-Lösungen abseits zentraler IT-Strukturen befeuert wird.

Mit dem Aufbau von Schweizer Cloud-Rechenzentren treten die grossen Anbieter den Zweiflern an der Datenhoheit und -souveränität ausländischer Cloud-Anbieter infolge des US CLOUD Act und der nachgelagerten Schrems Urteile entgegen. In der Praxis wird aber weiterhin vorsichtig gehandelt, da vereinzelte Services und Features nach wie vor von den globalen Datenzentren erbracht werden. Im Zweifelsfall sind die Daten «at rest» in einem Schweizer Datenzentrum, «in transit» jedoch kurzfristig in der EU oder sogar in den USA gewesen. Neue Funktionalitäten und Services werden in Schweizer Datenzentren zudem häufig nachträglich eingeführt. Besonderes Augenmerk erfordern auch die Business Continuity und das Disaster Recovery Failback, denn die grossen Hyperscaler sichern ihre Clouds mit mehrfachen Redundanzen ab, zumeist über Ländergrenzen hinweg. Entsprechend ist es ratsam, vorgängig genau zu prüfen, aus welchem Land die genutzten Services und Funktionalitäten im Normalfall und im Notfall bereitgestellt werden. Die gewonnenen Erkenntnisse sind in der Risikobetrachtung entsprechend zu berücksichtigen. Im Kontext des US CLOUD Act spielt auch die Thematik des «lawful access» eine zentrale Rolle.

Dieses Risiko hat jedoch, gemäss der öffentlich verfügbaren Datenquellen und der Anbieter, die sich der Sprengkraft eines solchen Eingriffs bewusst sind, eine geringe Eintrittswahrscheinlichkeit und lässt sich mit technischen, organisatorischen und vertraglichen Massnahmen auf ein vernünftiges Mass reduzieren.

Es ist erfolgskritisch, dass eine strategische Entscheidung, personenbezogene Daten, Kunden- oder Geschäftsdaten zu einem Cloud Provider auszulagern, auf einer soliden Grundlage erfolgt. Hierzu empfiehlt sich folgendes Vorgehen:

1. Erstellung einer fundierten Risikoanalyse, die sowohl das Institut und den Provider als auch die genutzten Services und Features miteinbezieht
2. Abbildung der Risiken anhand des Risikoappetits der Geschäftsleitung
3. Identifizierung und Umsetzung der erforderlichen technischen, organisatorischen und vertraglichen Massnahmen
4. Kontinuierliche Überwachung der identifizierten Risiken und Definition von wirkungsvollen Gegenmassnahmen

Abbildung 5: Umsetzung von Public Cloud Lösungen

Für Finanzinstitute spielt zudem die bestehende IT-Infrastruktur-Landschaft eine wichtige Rolle. Die zentralen Kernsysteme in Banken und Versicherungen laufen vielfach auf ganz spezifischer Hardware, wie beispielsweise auf Mainframes. Da sich insbesondere solche Systeme schlecht virtualisieren lassen, kommt eine Cloud-Migration dieser Server vorerst nicht infrage. Zusätzlich sind die Stabilität und Verfügbarkeit dieser Systeme von höchster Priorität. Moderne Konzepte wie Continuous-Deployment kommen bei Kernsystemen bisher nicht zum Einsatz, da selbst kleine Softwarefehler immense Auswirkungen haben können. Zum Zeitpunkt des Roll-outs muss die Maturität bereits sehr hoch sein, ein «Minimal Viable Product (MVP)» bringt in diesem Kontext häufig nicht die nötige Reife für einen produktiven Einsatz.

Dies hat zur Folge, dass Finanzinstitute weiterhin mit einer Two-Speed-IT unterwegs sind: mit Mainframes und eher langsamen, quartalsweisen Release-Zyklen. Die typischen Vorteile einer SaaS-Lösung lassen sich daher nur schlecht nutzen. Entsprechend muss die Architektur der Kernanwendungen vor einer Cloud-Migration neu definiert werden. Viele Banken und Versicherungen sowie auch deren Softwareanbieter stehen hier noch ganz am Anfang. Auf der anderen Seite der Two-Speed-IT stehen Portale, Apps oder auch Analytics-Anwendungen. Gerade hier zeigen sich die Vorteile der Cloud auch im Finanzumfeld. Neue Technologien wie beispielsweise künstliche Intelligenz sind ohne grosse Investitionen in eigene Hard- oder Software möglich. Die Analyse von grossen Datenmengen in Echtzeit mithilfe von Cloud-Rechenleistung ermöglicht innovative Beratungsdienstleistungen für Kunden oder die Automatisierung von komplexen Compliance- und Risk-Prozessen. Auch die Entwicklung und das Testen von neuen Applikationen ist damit schneller und effizienter möglich. Last- und Performance-Tests lassen sich mit temporären Cloud-Ressourcen kostengünstig durchführen. Flexibilität und Agilität reduzieren die Time-to-Market.

Die Cloud eignet sich im Finanzumfeld primär für Themen, die agile und kurzlebige Entwicklungen ermöglichen, während die vom Institut selbst betriebenen Kernsysteme auf der eigenen Infrastruktur verbleiben. Bei komplexen Backoffice-Anwendungen, mit denen sich ein Institut wenig differenzieren kann, ist jedoch ein Trend zum Outsourcing und zum Einsatz von SaaS-Applikationen zu beobachten. Dazu zählen beispielsweise CRM, Accounting/Rechnungswesen oder Office-Anwendungen. Voraussetzungen dafür sind modulare Systeme, auf denen einzelne Komponenten rasch weiterentwickelt werden können, ohne die Stabilität des ganzen Systems zu gefährden. Von zentraler Bedeutung sind ferner Cloud-taugliche Schnittstellen, um die Umsysteme zu verbinden.

Fazit: Public Clouds können im Finanzumfeld verstärkt eingesetzt werden.

Aus regulatorischer Sicht ist ein entsprechender Rahmen gesetzt und anhand der Risikoüberlegungen können Gegenmassnahmen festgelegt werden, welche die damit verbundenen Risiken tragbar machen. Wichtig ist, die Entscheidung für oder gegen ein spezifisches Cloud-Outsourcing mit entsprechender Sorgfalt zu prüfen, mit einem angemessenen Risikoentscheid zu dokumentieren und die Umsetzung auf Basis adäquater Massnahmen bewusst zu vollziehen. Dies gelingt am besten, wenn unter den relevanten Vertretern aus Business, IT, Risk, Compliance und Legal innerhalb des Instituts ein gemeinsames Verständnis der Cloud-Zukunft herrscht.

Die «Early Adopters» unter den Schweizer Finanzinstituten befinden sich bereits heute in der Betriebsphase, viele weitere in der strategischen Entscheidungsphase oder in konzeptionellen Überlegungen. Damit zeigt sich, dass die Vorteile von Public-Cloud-Umgebungen von Schweizer Finanzinstituten zunehmend anerkannt und genutzt werden. Institute, die diesen Technologie- und Innovationssprung nicht schaffen, werden mittel- bis langfristig das Nachsehen haben.

Cloud im regulierten Umfeld

Ein Interview mit Richard Hess

Wie würden Sie Ihre Rolle bei der Schweizerischen Bankiervereinigung, kurz SBVg, beschreiben?

Richard Hess: Seit Juli 2020 darf ich die Leitung des Bereichs Digitalisierung verantworten. Auf jeden Fall würde ich diese Rolle als vielseitig, interdisziplinär und bereichernd bezeichnen. Es vergeht kaum ein Tag, an dem ich nicht einen Aha-Moment erlebe und etwas Neues dazulernen darf. Im Fokus unserer Arbeiten stehen Fragestellungen und Herausforderungen, die sich im Kontext der Digitalisierung an der Schnittstelle von Technologie und Regulierung für die Finanzwirtschaft ergeben. Hierfür erarbeiten wir gemeinsam mit unseren Mitgliedern die notwendigen Grundlagen und Lösungsansätze, indem wir die richtigen Fragen stellen, die richtigen Experten zusammenbringen und die Koordination der entsprechenden Arbeiten in den Gremien übernehmen. In diesem Kontext übernehmen wir auch die Rolle als Bindeglied zwischen Finanzindustrie, Behörden und weiteren wichtigen Stakeholdern, wie beispielsweise grösseren Technologieunternehmen.

«Eine Welt ohne Risiko gibt es nicht. Deshalb ist die Versachlichung der Cloud-Diskussion für mich von zentraler Bedeutung.»

Richard Hess, Leiter Digitalisierung bei der SBVg

Erfahrungsgemäss lassen sich aber viele der aufkommenden Fragestellungen nicht immer im klassischen Schema «Problem-Lösung» angehen. Oftmals geht es auch darum, die Opportunitäten einzelner Trends für den Finanzplatz frühzeitig zu erkennen und diese aus Branchensicht aktiv zu begleiten, ohne immer eine konkrete Lösung für ein spezifisches Problem anzugehen. Beispiele sind Open Finance oder auch die Tokenisierung von Vermögenswerten. Das verbindende Ziel all dieser Aufgaben ist, dass unsere Mitglieder optimale Rahmenbedingungen in der Schweiz vorfinden, indem wir unternehmerische Freiräume schaffen und Innovation ermöglichen.

Zurzeit setzen wir uns dabei vor allem mit den Chancen und Herausforderungen von Open Finance, verantwortungsvoller Künstlicher Intelligenz, elektronischer Identität, digitalen Währungen (CBDC) oder auch Digitalen Vermögenswerten (Digital Assets) und DLT auseinander. Auch die verschiedenen regulatorischen Aspekte bei der Nutzung von Public-Cloud-Dienstleistungen durch Banken sind in unserem Fokus. Wir haben als SBVg bereits 2019 einen entsprechenden Leitfaden für unsere Mitglieder veröffentlicht.

Was sind aus Ihrer Sicht die Trends für die Nutzung von Cloud-Services?

RH: Eine kürzlich veröffentlichte Studie der SBVg zu den «Perspektiven zur Zukunft des Schweizer Banking» hat klar ergeben, dass Cloud Computing zu den Schlüsselressourcen der Zukunft gehört. Die Banken wollen Cloud-Services einsetzen und erkennen den daraus resultierenden Nutzen.

Gemäss den Erkenntnissen aus der Studie ist die Cloud-Journey im Finanzsektor zurzeit noch stark auf Infrastruktur fokussiert (Infrastructure-as-a-Service, IaaS), während die Geschäftsfähigkeit, Applikationen, Middleware, Daten-

banken und Entwicklungsplattformen sehr oft weiterhin in der Bank betrieben werden. Der Blick in die Zukunft zeigt jedoch, dass Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) stark an Bedeutung gewinnen werden. Auch Banking-as-a-Service (BaaS) wird schon aktiv gehandhabt. Die Studie des Bundes zur «Bedarfsabklärung Swiss Cloud» ist in diesem Kontext sehr hilfreich, da sie diesen Trend bereits quantifizieren konnte.

Im Office-Bereich haben die Banken, z. B. aufgrund der zunehmenden Nutzung von Kollaborationstools wie Microsoft Teams, bereits einige Touchpoints mit der Public Cloud. Interessant wird es aber vor allem dann, wenn Banken ganze Workloads aus ihren Geschäftsbereichen in die Public Cloud migrieren.

Nicht zuletzt haben auch die Aktivitäten von globalen Hyperscalern wie Microsoft und Google, die seit 2018 auch in der Schweiz eigene Datenzentren unterhalten, dazu beigetragen, dass sich Banken stärker mit dem Thema Cloud auseinandersetzen.

Was sind die zugrundeliegenden Treiber für die zunehmende Nutzung von Cloud-Services?

RH: Hier erachte ich insbesondere das Marktumfeld und die sich wandelnden Kundenbedürfnisse als wesentliche Treiber. Smartphones sind ja nicht mehr aus unserem Alltag wegzudenken. Gleichzeitig verändern neue Mitbewerber und Challenger-Banken die Erwartungshaltung der Kundinnen und Kunden an Finanzdienstleistungen. Schnell, einfach und sicher ist hier die Devise. Um in diesem Wettbewerb mithalten zu können, ist eine kurze Time-to-Market erfolgsentscheidend. Dies stellt für viele Banken mit älteren Legacy-Systemen eine Herausforderung dar. Vor diesem Hintergrund kann die Cloud die Banken befähigen, die sich wandelnden Kundenbedürfnisse noch besser zu erfüllen und wird damit zu einem Enabler für innovative Geschäftsmodelle. Zudem sind viele der neuen Technologien nur über eine Cloud sinnvoll nutzbar. Nicht zuletzt hat auch die Corona-Pandemie die Nachfrage der Banken nach Cloud-Dienstleistungen weiter beschleunigt, da beispielsweise die meisten virtuellen Kollaborationstools nur aus der Cloud als SaaS verfügbar sind.

Wie gestalten sich die Rechtslage und die regulatorischen Rahmenbedingungen in Bezug auf die Cloud-Nutzung?

RH: Das ist sicherlich die Kernfrage für uns. Grundsätzlich bietet das herrschende Prinzip der technologieneutralen und prinzipienbasierten Regulierung in der Schweiz genügend Flexibilität, um Cloud-Dienstleistungen im bestehenden Rahmen zu nutzen. Dies bedingt aber eine konkrete Interpretation geltender rechtlicher und regulatorischer Anforderungen im Cloud-Kontext. Mit unserem Cloud-Leitfaden haben wir hierzu eine Reihe von Empfehlungen ausgearbeitet. In diesem Sinne ist die aktuelle Rechtsgrundlage aus unserer Sicht verständlich und ausreichend praktikabel. Es gibt aber weiterhin noch nicht vollständig gelöste Punkte. Beispielsweise ist der Umgang mit der Datenherausgabepflicht der Cloud Provider an Dritte basierend auf dem US CLOUD Act nach

wie vor eine umstrittene Frage ohne abschliessende Antwort – auch unter Fachleuten. Ein weiterer wichtiger Punkt im Hinblick auf das Risikomanagement ist das Schrems II-Urteil. In der Konsequenz müssen die Banken ihren Cloud Provider sowie dessen Subunternehmer nicht nur kennen, sondern auch genau wissen, wohin die Daten fliessen, wo ihre Daten aufbewahrt werden und wer auf diese zu welchem Zweck zugreifen und diese gegebenenfalls bearbeiten kann.

Wie ist das Feedback Ihrer Mitglieder zum Cloud-Leitfaden?

RH: Der Leitfaden wird nach unserem Wissen von vielen Mitgliedern als hilfreich angesehen und bei der eigenen Umsetzung von Cloud-Strategien als Hilfestellung herangezogen. Wir hören von unseren Mitgliedern auch, dass mithilfe des Leitfadens die Diskussionen innerhalb der Institute und mit den Cloud-Anbietern sofort auf die zentralen Themen fokussiert werden können. Das ist erfreulich, denn genau dafür haben wir ihn auch verfasst. Nach meiner Einschätzung hat er auch dazu beigetragen, das Dogma «Nein zur Public Cloud» aus der Welt zu schaffen oder zumindest zu relativieren und die Cloud-Diskussion zu versachlichen.

Gegenstand des Leitfadens sind Empfehlungen, welche bei Beschaffung und beim Einsatz von Cloud-Dienstleistungen durch Banken und die Cloud-Anbieter herangezogen werden können. Insgesamt werden vier Bereiche beleuchtet: Hilfestellungen zur Datenbearbeitung, für die Zusammenarbeit mit Subunternehmern, für Audits sowie für den Umgang mit Datenherausgabeanordnungen von internationalen Behörden. Insbesondere werden Empfehlungen zu technischen, organisatorischen und vertraglichen Massnahmen mit Blick auf den Datenschutz und die Einhaltung des Bankgeheimnisses in der Cloud gegeben.

Was sind aus Ihrer Sicht die grössten Herausforderungen in Bezug auf Cyber Security & Privacy bei der Cloud-Adaptierung?

RH: Klar ist, dass die Bedeutung von Cyber Security – beispielsweise auch im Kontext von Open Banking und dem damit verbundenen verstärkten Austausch von Daten mit Dritten – laufend an Bedeutung gewinnt. Auf Branchenebene adressieren wir das Thema, indem wir beim Aufbau eines Kompetenzzentrums für Cybersicherheit gemeinsam mit dem Bund mitwirken.

Weiter sind im Cloud-Kontext vor allem der Ort der Datenspeicherung sowie die Datensouveränität zentral. Das heisst: Wie behalte ich die Hoheit über meine Daten und welche Mittel habe ich, um meine diesbezüglichen Rechte durchzusetzen? Transparenz ist in diesem Kontext ein wichtiger Aspekt.

Wie schätzen Sie die Verfügbarkeit und Entwicklung der benötigten Fähigkeiten Ihrer Mitglieder in Bezug auf die Umsetzung von Cloud-Vorhaben ein?

RH: Das hängt davon ab, von welchen Instituten wir sprechen. Banken werden bekanntlich mehr und mehr zu Technologieunternehmen. Der Trend geht gemäss vielen Fachleuten dahin, dass Bankenmitarbeitende in Zukunft mehr Technologie-Skills besitzen und umgekehrt IT-Mitarbeitende mehr vom Business verstehen müssen. Der «War for Talents» für spezifische IT-Skills, gerade im Cloud-Bereich, ist daher sicherlich auch im Finanzbereich spürbar. Hier stehen die Banken in direktem Wettbewerb mit Technologieunternehmen und müssen sich entsprechend positionieren, um als Arbeitgeber attraktiv zu bleiben. Gerade für kleinere und mittlere Banken könnte es eine grössere Herausforderung darstellen, eine eigene IT-Organisation zu unterhalten, die mit allen rechtlichen, risikobasierten und technischen Fragestellungen Schritt halten kann. Eine mögliche Stossrichtung wären Kooperationen mit Drittanbietern und die Aufsplittung der Wertschöpfungskette. Hier sind wir bestrebt, unsere Mitglieder bei der Aus- und Weiterbildung ihrer Mitarbeitenden bestmöglich zu unterstützen, beispielsweise durch die Kooperation mit ausgesuchten Weiterbildungsplattformen.

Wo sehen Sie zusätzliches Potenzial durch die Cloud-Adaptierung?

RH: Ein starkes Argument für die Nutzung der Cloud sind die Themen Künstliche Intelligenz (KI) und Machine Learning (ML). Der Einsatz von KI und ML bietet den Banken völlig neue Möglichkeiten, grosse und qualitativ hochwertige Datenmengen aufzubereiten und bereitzustellen. Hinzu kommen die «On-Demand» verfügbare Computing Power, die direkt von den Hyperscalern bezogen werden können – beispielsweise für das Transaction Monitoring oder für die Fraud Detection. Nicht zuletzt spielen auch Sicherheitsaspekte eine wesentliche Rolle, wieso sich Banken für einen Gang in die Cloud entscheiden.

Was sind aus Ihrer Erfahrung die relevanten Elemente einer Cloud-Strategie in Ihrer Organisation/ Branche?

RH: Hier gilt es, zwischen inlandorientierten und globalen Banken zu differenzieren. Beide haben unterschiedliche Ausgangslagen und Bedürfnisse. Banken, die auf den inländischen Markt fokussieren, sind eher an lokalen Anbietern aus der Schweiz interessiert und haben weniger komplexe Strategien. Globale Banken hingegen setzen sich mit dem Thema erfahrungsgemäss viel umfassender auseinander. Häufig werden Cloud-Strategien in diesem Umfeld auch vom Mutterhaus definiert und in den einzelnen Ländern ausgerollt.

Die Frage, die unabhängig von der Grösse der Bank immer wieder diskutiert wird, lautet: Ist Cloud ein IT- oder ein Business-Thema? Aus meiner Sicht muss die Cloud-Transformation zwingend als strategisches Projekt gesehen und auf Geschäftsleitungsebene diskutiert werden. Entscheidungen für oder gegen die Cloud sowie der Risikoappetit sind auf dieser Ebene zu treffen.

Für die Umsetzung ist es aus Gesprächen mit Bankenvertretern wichtig, dass der Grundsatz «Cloud First» den Transformationsprozess begleitet, der sich in der Regel über mehrere Jahre entlang des IT-Lifecycles erstreckt. Zusätzlich braucht es eine klare Vision und Grundsätze sowie ein kritisches Hinterfragen im Falle von Abweichungen von diesem Grundsatz. Auch die organisatorischen Auswirkungen der Cloud-Migrationen sind nicht zu vernachlässigen und unbedingt zu berücksichtigen.

Ein unabdingbarer Punkt für die Cloud-Strategie, gerade im Finanzsektor, sind aus meiner Sicht auch regulatorische Aspekte. Hier geht es wie erwähnt darum, dass bereits im Rahmen der Strategieentwicklung alle Fragen in Bezug auf den Cloud-Anbieter und dessen Subunternehmer beantwortet werden sollten. Auch eine klare Antwort auf die Frage «Wer kann wann, wie und zu welchem Zweck auf welche Daten zugreifen?», ist aus Risikosicht unerlässlich. Eine Provider-Entscheidung sollte erst dann gefällt werden, wenn alle genannten Punkte geklärt sind.

Gibt es sonst noch etwas, das Sie unseren Leser*-innen gerne mit auf den Weg geben möchten?

RH: Eine Welt ohne Risiko gibt es nicht. Deshalb erachten wir die Versachlichung der Cloud-Diskussion als wichtig. Denn dieser Schritt bedeutet keinesfalls, dass sich eine Organisation von einer «Zero-Risk»-Welt hin zu einem Hochrisiko-Umfeld bewegt. Eine Vielzahl von Risiken existieren auch bereits für Applikationen, die vor Ort in eigenen Rechenzentren betrieben werden. Was es braucht, ist einen risikobasierten Zugang zu den relevanten Fragestellungen rund um die Cloud. Banken, die alle potenziellen Risiken sorgfältig abwägen, bietet die Cloud eine grosse Chance, ihre Innovations- und Wettbewerbsfähigkeit zu steigern.

Unsere Ambition ist es, sicherzustellen, dass alle Banken, die in die Public Cloud wollen, dies auch können. Dabei sind wir sehr gespannt, wohin die Reise in den nächsten Jahren gehen wird. Schliesslich bewegen wir uns hier in einem sehr dynamischen und sich rasch entwickelnden Umfeld, das nicht nur technische und regulatorische Fragen aufwirft, sondern in letzter Instanz auch geopolitische, die es zu berücksichtigen und zu diskutieren gilt.

Cloud im öffentlichen Sektor – ein dringendes Gebot mit viel Potenzial

Der öffentliche Sektor umfasst Organisationen über alle föderalen Stufen, insbesondere die öffentliche Verwaltung, die Bildung und Forschung, Sicherheitsorganisationen sowie öffentliche Energieversorger, Transport- und Logistikunternehmen. Mit seiner Grösse könnte dieser Sektor ein Schwergewicht der Cloud-Transformation werden. Doch zurzeit ist die Nutzung noch gering.

Marc Raum, Thomas Vogt

Für den öffentlichen Sektor gilt das in der Bundesverfassung (BV) verankerte Legalitätsprinzip, das für staatliches Handeln formalrechtliche Grundlagen fordert (Art. 5 Abs. 1 BV). Dabei nehmen im Wesentlichen die Parlamente und im gesetzten Vollzugsrahmen die Verwaltung in Eigenverantwortung die Rolle des Regulators wahr. Damit sind grundsätzlich viele Vorgaben auf Basis von Gesetzen und Verordnungen vorhanden. Ihre konkrete Auslegung in Bezug auf die Möglichkeiten und Einschränkungen der Cloud-Nutzung ist jedoch selten eindeutig. Die öffentlichen Aufsichtsorgane, z. B. für den Datenschutz, verweisen zwar auf die Risiken, bieten aber selbst keine Lösungsansätze an.

Der Einsatz von Cloud-Services ist für den öffentlichen Sektor auch ein politisches Thema, insbesondere unter dem Aspekt der Datensouveränität im internationalen Kontext. Damit hat sich die Schweizer Regierung unter anderem mit ihrer «Swiss Cloud»-Machbarkeitsstudie im Jahr 2020 auseinandergesetzt. Diese ergab, dass kein oder nur ein sehr geringer Bedarf an einer eigenen, durch den Bund betriebenen Cloud-Infrastruktur vorhanden ist, aber ein grosser Bedarf an klaren Rahmenbedingungen zur Nutzung von kommerziellen Cloud-Services existiert. Für die Schaffung dieser Rahmenbedingungen sieht die Bedarfserhebung einerseits die öffentlichen Organe sowie insbesondere die Branchenverbände und die entsprechenden Regulatoren in der Pflicht.

Die öffentliche Hand hat es bislang verpasst, regulatorische Klarheit zur Nutzung von Public-Cloud-Services zu schaffen. In Zusammenarbeit mit den Branchenverbänden könnten jedoch problemlos praxistaugliche Hilfsmittel und Angebote entstehen.

Trends und Treiber für die Cloud-Nutzung im öffentlichen Sektor

Die Cloud-Nutzung ist für den öffentlichen Sektor insbesondere in Anwendungsbereichen interessant, wo die Cloud-Fähigkeiten einen direkten Mehrwert erbringen und die Rahmenbedingungen bezüglich Datenhaltung und -verarbeitung für die Cloud-Nutzung klar definierbar sind. Hierzu gehören beispielsweise:

- Portale und Anwendungen (beziehungsweise Mobile-Apps) für die direkte Bereitstellung von Dienstleistungen für die Bevölkerung und private Unternehmen
- Anwendungen mit einem unstetigen Ressourcenbedarf, die rasch skalierbar sein müssen
- Services, die einen Datenaustausch mit externen Stakeholdern beinhalten beziehungsweise ermöglichen sollen (z. B. Open Government Data Services)
- Spezifische Anwendungen, die Fähigkeiten bereitstellen, die einer konstanten technologischen Weiterentwicklung unterworfen sind, wie beispielsweise Services in den Bereichen Data Analytics, Machine Learning oder Artificial Intelligence

Konkrete Beispiele für die Nutzung von Public Cloud Services im öffentlichen Sektor sind die Verwaltung und Bereitstellung der Schweizer Landestopografie-Karten durch swisstopo, die Covid-Tracing-App des Bundesamts für Gesundheit BAG, die Test- und Entwicklungslösungen zur agilen Entwicklung sowie die Nutzung von Cloud-Lösungen in der internen und organisationsübergreifenden Kommunikation und Kollaboration in vielen öffentlichen Verwaltungen.

«Death by a thousand cuts»

Der Weg zur Nutzung von Cloud-Lösungen durch die öffentliche Hand ist in der Regel sehr steinig. Neben den auch politisch ungeklärten Rahmenbedingungen zur Nutzung von Cloud-Services im öffentlichen Sektor, insbesondere bei der Informationssicherheit und beim Datenschutz, muss hierzu eine hohe Hürde überwunden werden. Das öffentliche Beschaffungswesen fordert rasch eine Ausschreibung mit neuen Verträgen für die Leistungen, die damit bereits ein sehr präzises Verständnis des künftigen Betriebsmodells, der Compliance-Anforderungen und des Bedarfs erfordert. Dies wiederum setzt reife Architekturgrundlagen voraus, speziell im Bereich der Integration, der Netzwerke und der Sicherheitssysteme, damit die Public Cloud Services auch effektiv genutzt werden können. An diesen Voraussetzungen scheitern viele kleinere Stellen.

Dieser kleinteilige, fragmentierte Ansatz führt dazu, dass einzelne Stellen kaum die Wirtschaftlichkeitsschwelle erreichen, um sich intern die erforderliche Finanzierung zu sichern. Doch die Situation bessert sich. Mit der SBB, der Post und der Bundesverwaltung haben sich drei grosse Organisationen entschieden, Public Cloud Services zu beschaffen. Diese Erfahrungen werden sich als wertvoll erweisen, da es nun Vorbilder gibt, wie man es macht. Gleichwohl braucht es ein strategisch abgestimmtes Vorgehen, um den Nutzen von Cloud Services zu erschliessen.

Mögliches Zielbild für die Cloud-Nutzung im öffentlichen Sektor

Als Basis für eine sichere, regelkonforme und effiziente Nutzung von Cloud Services benötigen Organisationen des öffentlichen Sektors eine politisch belastbare und breit abgestützte Organisationsentwicklung mit strategischen Prinzipien, die als Leitplanken für die Cloud-Integration und -Nutzung fungieren. Dabei ist es empfehlenswert, das Thema Cloud aus organisatorischer Sicht nicht losgelöst zu betrachten, sondern als wesentlicher Baustein resp. Enabler für die digitale Transformation.

Aus unserer Sicht gibt es im Wesentlichen folgende entscheidende Elemente für eine aktive und nachhaltige Cloud-Transformation im öffentlichen Sektor:

- Vorhandene Erfahrungen sichtbar machen

- Anwendungsorientierte Grundlagen im Bereich Architektur, Informationssicherheit und Datenschutz schaffen
- Bedarf bündeln durch eine formalisierte Zusammenarbeit verschiedener Stellen und flexible Beschaffungsgrundlagen, indem beispielsweise Synergiepotenziale via IT Service Provider erschlossen werden
- Politischen Prozess einleiten und Zielbild mit Anwendungsszenarien sowie einen ambitionierten Zeitplan verabschieden
- Wechsel zu agilen und iterativen Vorgehensweisen wie Scrum und SAFe, um eine fehlertolerante Lernkultur zu verankern – die Organisation dabei laufend überprüfen und anpassen
- Aus- und Weiterbildung der Mitarbeitenden hinsichtlich der benötigten Cloud-Fähigkeiten, -Modelle und -Technologien
- Etablierung und Kollaboration in nationalen und internationalen Cloud-Initiativen zur Bündelung und Fokussierung der Expertise und Entscheidungsgrundlagen im Kontext der Cloud-Transformationen im öffentlichen Sektor

Abbildung 6: Empfohlene Elemente für eine erfolgreiche Cloud-Transformation

Ein möglicher Ansatz, um der Cloud-Nutzung im öffentlichen Sektor in der Schweiz den erforderlichen Schub zu geben, ist eine gezielte und koordinierte Initiative für das Thema. Beispiele von Cloud-Initiativen in der öffentlichen Hand sind die UK Government G-Cloud, das FedRAMP der US-Regierung, die cloud.gov.au der australischen Regierung oder die Government Commercial Cloud (GCC) von Singapur. Bei der G-Cloud der britischen Regierung handelt es sich primär um klar definierte Rahmenbedingungen zur erleichterten Beschaffung von Cloud-Dienstleistungen. Das FedRAMP der US-Regierung geht noch einen Schritt weiter und stellt einen Zertifizierungsprozess bereit, der eine standardisierte Risiko- und Sicherheitsbetrachtung von Cloud Services sicherstellt. Dadurch kann rasch und nachvollziehbar entschieden werden, ob, und wenn ja, welche Cloud-Services für einen bestimmten Anwendungsfall eingesetzt werden dürfen. Die australische Regierung hat mit ihrer cloud.gov.au Initiative strategisch festgelegt, dass ICT-Leistungen der Verwaltung generell cloudtauglich konzipiert werden müssen. Die GCC der Regierung von Singapur ermöglicht die Nutzung von innovativen Cloud Services für sensitive Anwendungsbereiche der Verwaltung.

Mit GAIA-X ist in Europa eine grosse Cloud-Initiative gestartet worden, die ähnliche Bereiche wie die bereits erwähnten Initiativen adressiert und auf jeden Fall auch vom öffentlichen Sektor in der Schweiz intensiv mitverfolgt werden sollte. Insbesondere die Fähigkeit von GAIA-X, Cloud Services in verschiedenen Serviceklassen anzubieten resp. auszuweisen, kann für die Cloud-Nutzung im öffentlichen Sektor sehr hilfreich sein. Auch der Bericht zur Bedarfsabklärung für eine Swiss Cloud[1] des Bundesrates hat mit der Handlungsempfehlung zur Prüfung eines Zertifizierungssystems für Cloud Services diese Stossrichtung adressiert.

Der öffentliche Sektor hat im gesamten Themenkomplex der Cloud-Transformation noch wertvolles Potenzial, um mit Kooperationen zwischen den verschiedenen Organisationen und föderalen Stufen hinweg zusätzliche Synergien freizusetzen. Da viele Fragestellungen zur Cloud in den verschiedenen Organisationen des öffentlichen Sektors ähnlich gelagert sind, empfiehlt sich eine offene und intensive Zusammenarbeit. Ebenso wichtig ist die gemeinsame Erarbeitung von belastbaren Entscheidungsgrundlagen, welche die Cloud-Transformation und damit auch die gesamte digitale Transformation der einzelnen Organisationen einen grossen Schritt voranbringen.

[1] https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

Vorreiter beim Bund
in der Nutzung von Public Cloud Services

Hanspeter Christ hat einen Abschluss als Kulturingenieur der ETH Zürich und arbeitet seit dem Jahr 2000 beim Bundesamt für Landestopografie swisstopo. Seit 2004 beschäftigt er sich bei swisstopo mit der Konzeption, dem Aufbau und Betrieb von mehrheitlich aus Open-Source-Komponenten bestehenden Geodaten-Infrastrukturen. Bereits 2008 sammelte er erste Erfahrungen in der Nutzung von Public Cloud-Services und trieb in den folgenden Jahren die Cloud-Konzeption und -Migration der gesamten Geodaten-Infrastruktur des Bundes in die Public Cloud an vorderster Front voran.

«Unsere Reise in die Cloud führte uns von einer On-Premises betriebenen Infrastruktur über eine hybride Architektur zu einer heute weitgehend cloudbasierten Implementierung des Geoportals.»

«Wir hatten 2008 eine dringende Kundenanfrage für die Nutzung des digitalen Kartenmaterials von swisstopo auf dem Tisch. Hätten wir hierzu eine eigene Infrastruktur nach traditionellem Ansatz beschafft und integriert, wäre zum gewünschten Go-live-Termin nicht einmal die erforderliche Hardware rechtzeitig verfügbar gewesen.»

Die Treiber für die Cloud-Nutzung bei swisstopo waren der Bedarf an einer flexiblen Infrastruktur, die sich den jeweiligen Bedürfnissen der Geoportal-Nutzung möglichst gut anpasst sowie hochskalierbare Map Services. Die damit einhergehende Cloud-Transformation von swisstopo umfasste zunächst die Migration auf eine hybride Architektur, die sowohl interne Infrastrukturressourcen als auch Public-Cloud-Ressourcen nutzte. Im nächsten Schritt wurde die Geoportal-Architektur dann zu einer heute weitgehend cloudbasierten Infrastruktur weiterentwickelt.

Dieses Vorgehen prägt auch unsere neue Herangehensweise: *«Wir definieren keine Wunsch-Infrastrukturen und -Architekturen auf dem Reissbrett, sondern verfolgen den Markt und fokussieren dabei gezielt auf «Low-hanging Fruits» mit grossem Nutzenpotenzial.»*

Empfehlungen an öffentliche Organisationen für Migrationen in die Public Cloud

- Mit einer reinen Migration von virtuellen Maschinen in die Public Cloud (Lift-and-Shift) lassen sich die Vorteile der Cloud-Fähigkeiten nicht vollständig ausschöpfen. Die Nutzung optimierter Cloud-Lösungsmuster – beispielsweise mit Microservice-Architekturen – ermöglicht die Erschliessung von wesentlich grösseren Potenzialen. Grenzen für viele Nutzerorganisationen setzen anbieterspezifische Services, die eine spätere Migration erschweren. Standardisierte Architekturprinzipien helfen hier, nachhaltige Entscheidungen sicherzustellen.

- Eine Kultur des produktiven Experimentierens mit neuen Technologien erlaubt, hohe Effizienzgewinne zu realisieren in der Entwicklung und im Betrieb von IT-Lösungen. Hierzu eignen sich agile Arbeitsweisen, wie beispielsweise SAFe, die mit Innovations- und Planungssprints dafür sorgen, dass das Erkunden neuer Ansätze zum Alltag wird.

Cédric Moullet studierte an der EPFL und besitzt einen MBA der Haute École de Gestion in Fribourg sowie einen CAS in Artificial Intelligence der Fachhochschule Bern. Er begann seine berufliche Laufbahn an der ETH Zürich. Anschliessend arbeitete er für den amerikanischen Softwareentwickler Autodesk und die Open-Source-Softwarefirma Camptocamp, die ihn zu swisstopo sowie danach zum Bundesamt für Informatik und Telekommunikation BIT führte. Dort hat er zuletzt die Entwicklung der SwissCovid App sowie des Covid-Zertifikates geleitet. Seit dem 1. September 2021 verantwortet Cédric Moullet das Ressort Digitalisierung & IT beim Schweizer Alpen-Club SAC.

«Ein kritischer Erfolgsfaktor für eine effiziente, sichere und nachhaltige Adaptierung von Public Cloud Services ist der Aufbau der benötigten Fähigkeiten der Mitarbeitenden im Cloud-Bereich an den unterschiedlichen Positionen einer Organisation.»

Die einschlägigen Cloud-Erfahrungen bei swisstopo, wo Cédric als Leiter den Aufbau des Geoportals vorantrieb, konnte er während der Corona-Krise in die Entwicklung der SwissCovid Tracing-App und der Covid Certificate App einbringen. Man rechnete mit einer sehr hohen Anzahl von Zugriffen. Hierfür waren die eigenen Rechenzentren jedoch nicht ausgelegt. Gleichzeitig war es erfolgskritisch, dass die Bürger*innen der Lösung vertrauen. Diese Herausforderungen wurden mit einem hybriden Ansatz gelöst: Ein Content Delivery Network (CDN) bewältigt die Zugriffe flexibel. Die Grundfunktionen des Backends wurden in den eigenen Rechenzentren bereitgestellt. Zudem wurde der Code unter Open Source gestellt und einem Public-Security-Test unterzogen, damit sich alle von der Funktionsweise überzeugen konnten. Der CDN-Service hatte zudem den Vorteil, dass er sich sehr leicht einbinden liess und so die Bereitstellung der Lösung beschleunigte. Der Wissenstransfer zwischen den Spezialisten selbst nahm wenig Zeit in Anspruch. Zu reden gab, ob die IP-Adressen der Benutzer*innen Personendaten darstellen, da diese in Kombination mit dem Covidcode z. B. den Rückschluss zulassen, ob jemand krank war.

Cédrics Erfahrung nach ist die Technik aber nur ein Element der Sicherheit: *«Das schwächste Glied in der Kette ist oft der Mensch. Der Gang in die Cloud verstärkt diese Risiken.»*

Empfehlungen an öffentliche Organisationen für Migrationen in die Public Cloud

- Der Zugang zu einem Expertenpool hilft, Cloud-Lösungen richtig zu konzipieren und schnell zu realisieren. Das Ziel sollte darin bestehen, die internen Mitarbeitenden durch Wissens- und Verantwortungstransfer zu befähigen.

- Sicherheit und Vertrauen sind aktiv zu bewirtschaften. Sichere Architekturen und eine hohe Transparenz (z. B. durch Open Source und Audits) sind hierzu wichtige Bausteine.

Ihre Kontakte

Adrian Anderegg
Partner
adrian.anderegg@awk.ch

Marc Raum
Senior Manager
marc.raum@awk.ch

Thomas Vogt
Senior Manager
thomas.vogt@awk.ch

Tom Schons
Manager
tom.schons@awk.ch

AWK Group AG
Leutschenbachstrasse 45
CH-8050 Zürich
T +41 58 411 95 00
www.awk.ch

Zürich • Bern • Basel • Lausanne • Luxemburg

AWK Group
Enabling digital performance.

Über AWK

AWK Group ist eine unabhängige internationale Management- und Technologieberatung mit Standorten in Zürich, Bern, Basel, Lausanne und Luxemburg. Mit über 400 Mitarbeiter*innen begleitet AWK die digitale Transformation von Organisationen aus unterschiedlichsten Branchen von der Strategie bis zur Umsetzung und ist mit den Technologien der Zukunft vertraut. Ihre Dienstleistungen erstrecken sich von der Entwicklung digitaler Geschäftsmodelle über Data Analytics, Cyber Security und IT Advisory bis hin zum Management komplexer Transformationsprojekte.