

Public-Cloud-Computing für Versicherer – Mehr Effizienz, aber auch Komplexität



Claudio Stadelmann



Moritz Feuchter



Florian Gasser

Die Digitalisierung berührt nahezu alle Wirtschaftsbereiche und führt regelrecht zu einer Explosion des Datenaustauschs und einer damit verbundenen Datenflut. Die zunehmend digitale Welt eröffnet zwar neue datenbasierte Geschäftsmodelle für die Versicherungsindustrie, jedoch sind speziell in diesem Bereich die regulatorischen Anforderungen nicht zu unterschätzen. Public-Cloud-Computing für diese neuen Geschäftsmodelle zu nutzen, kann in diesem Zusammenhang zwar die Effizienz steigern, gleichzeitig aber auch zum Katalysator und Multiplikator von Komplexität werden, wenn im Vorfeld nicht die richtigen Weichen gestellt werden. Im vorliegenden Artikel diskutieren wir, welche Herausforderungen eine Public-Cloud-Lösung besonders für Versicherungsunternehmen mit sich bringt, welche Aspekte bei der Entscheidung berücksichtigt werden müssen und welche Massnahmen unternommen werden sollen, um die Risiken bei einer Umsetzung zu minimieren.

Wenn Daten lästig werden...

Die Digitalisierung an sich führt zu einer regelrechten Datenexplosion und einer zunehmenden Kommerzialisierung derselben. Die weltweite digitale Datenproduktion steigt nach einer Studie von Statista¹ von 16 Zettabyte im Jahr 2016 auf über 163 Zettabyte im Jahr 2025 an. Um es in anderen Worten auszudrücken: die prognostizierte digital verfügbare Byteanzahl wird im Jahre 2025 in etwa der 32-fachen Menge aller Sandkörner auf unserem Planeten entsprechen – Tendenz steigend.² Egal ob man als Person einen Versicherungsvertrag abschliesst³, sich zu wenig bewegt⁴ oder mit seinem Auto zu schnell fährt⁵ – es werden mittlerweile überall und jederzeit Daten generiert, die zu merkantil verwertbaren Informationen führen. Dies ruft nicht

zuletzt Datenschutzbehörden und Regulatoren auf den Plan.

Schöne neue Welt?

Zur besseren Operationalisierung der Datenflut entschlossen sich viele Versicherungsunternehmen dazu, Public-Cloud-Computing – also die Nutzung standardisierter und unter mehreren Kunden geteilter IT-Services im Internet⁶ – auf die strategische Agenda zu nehmen. Auch eröffnet die Public Cloud für (Rück-)Versicherungsgesellschaften zahlreiche neue Geschäftsmodelle und verbesserte Kooperationsmöglichkeiten, gerade auch im Verbund und der Zusammenarbeit mit Geschäftspartnern und Endkunden – wohlbemerkt bei gleichzeitiger Inaussichtstellung erhöhter Kosteneffizienz, etwa im Rahmen von «Economies of Scale»⁷. Getrieben von den Vorteilen⁸ von Betriebsmodellen wie «Software as a Service» (SaaS), «Platform as a Service» (PaaS) oder «Infrastructure as a Service» (IaaS) tritt Cloud-Computing in Konkurrenz zu traditionellen Betriebsmodellen. Abbildung 1 stellt schematisch die wesentlichen Elemente dar, auf welche sich die einzelnen Cloud-Kategorien fokussieren.

Bereits 2010 wurden von Versicherungsunternehmen SaaS-Lösungen in einer Studie des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation⁹ ein hoher Bekanntheitsgrad und grosses Entwicklungspotential attestiert. Neben reinen Kosteneinsparungen, die etwa aus einer schlankeren eigenen IT-Administration resultieren, kann sich für Versicherungsunternehmen nachhaltiges Wertschöpfungspotenzial auf der Grundlage einer ertragsschaffenden Interaktion zwischen Nutzern der Public-Cloud-basierten Plattform¹⁰ ergeben, vorausgesetzt natürlich, die sich

Die Autoren

Claudio Stadelmann ist Partner, Financial Services, bei BearingPoint.

Moritz Feuchter ist Senior Manager bei BearingPoint.

Florian Gasser ist Management Consultant bei BearingPoint.

ergebenden Möglichkeiten werden entsprechend genutzt.

Auf der Kehrseite der Medaille bedeuten Public-Cloud-Lösungen aber unter Umständen auch eine erhöhte Risikolage, verbunden mit grösserer gesetzgeberischer Aufmerksamkeit und entsprechendem aufsichtsrechtlichen Gestaltungswunsch. Um nur einige regulatorische und datenschutzrelevante Aspekte im Kontext des Public-Cloud-Computings zu beleuchten, sei angeführt, dass die dezentrale Datenlagerung und -bearbeitung ausserhalb der Schweiz die Anforderung nach sich zieht, im entsprechenden Land ein vergleichbares Datenschutzniveau vorzufinden.¹¹ Hierzu muss man zunächst Gewähr finden, wo genau in einer Public-Cloud-Umgebung die Daten überhaupt liegen, beziehungsweise von wo aus auf die Daten zugegriffen werden kann. Datenschutzrechtlich kann es keinen wesentlichen Unterschied machen, ob Daten an eine externe Stelle übermittelt werden oder ob ermöglicht wird, darauf von externer Seite zuzugreifen. Der datenschutzrechtliche Effekt auf die betroffenen Personen ist schlicht derselbe.

Die Querelen um die Vergleichbarkeit des Datenschutzniveaus lassen sich am Beispiel USA / EU bestens versinnbildlichen. Die im Jahre 2000 im Safe-Har-

bour-Abkommen getroffenen Vereinbarungen, die geschlossen wurden, um ein vergleichbares Datenschutzniveau zwischen der EU und den USA zu erreichen,¹² hat der Europäische Gerichtshof (EuGH) 2015 aus verschiedenen Gründen gekippt. In der Konsequenz bedeutete dies, dass von einer Gleichwertigkeit des Schutzniveaus nicht länger ausgegangen werden konnte. Um dieses Vakuum zu schliessen, wurde zwischen der EU und den USA neu verhandelt und das Data-Privacy-Shield-Abkommen¹³ unterzeichnet. Jedoch steht auch dieses Abkommen mit der Adaption des Privacy Acts durch die aktuelle US-Präsidentschaft auf tönernen Füßen und die Gerichtsfestigkeit dieses Abkommen ist keineswegs gesichert. Vielmehr ist nach dem Urteil des EuGH fraglich, ob die Zulässigkeit von Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen, erreicht werden kann.¹⁴

Unabhängig davon sind am 25. Mai 2018 die Regelungen der Datenschutzgrundverordnung (GDPR bzw. EU DSGVO)¹⁵ in Kraft getreten. Diese normiert den Umgang mit personenbezogenen Daten¹⁶ (sog. Personal Identifying Information, PII) von EU-Bürgern für Unternehmen und führt zusätzliche Trans-

parenz- und Verhaltensregeln ein. Gegenüber dem nationalen Recht in den Mitgliedsstaaten der Europäischen Union hat die GDPR Anwendungsvorrang.¹⁷ Zahlreiche Novellierungen zum Datenschutz in den einzelnen Mitgliedsländern führen dazu, dass die konkrete landesspezifische Umsetzung gerade hinsichtlich Cloud Computing zum Teil divergiert, da entsprechende Öffnungsklauseln Raum schaffen, Themenkomplexe abweichend zu regeln. Darüber hinaus kann die Kooperation mit einem Public-Cloud-Anbieter in der Schweiz eine durch die FINMA genehmigungspflichtige Änderungen des Geschäftsplans bedeuten.¹⁸

Die anhand dieser Beispiele aufgezeigten divergierenden und teilweise rasch wechselnden gesetzlichen Rahmenbedingungen lassen den Komplexitätsgrad erahnen, in welchem Datensysteme fehlerfrei operieren müssen – und das ganz unabhängig davon, ob sich diese «on premise» oder «in the cloud» befinden.

Trotzdem oder gerade deswegen haben noch nicht alle Versicherer ihren Weg hin zur Datenschutz-Compliance und einer Datenharmonisierung gefunden, da system- und auch gesetzestechisch noch einige Herausforderungen bestehen. Für Schweizer Versicherungsunternehmen sind dies unter anderem:

- Harmonisierung der gesetzlichen Vorgaben mit der (geplanten) technischen Umsetzung: Aktuell sind „Multi-Tenant“-Services kaum in der Lage, den Schweizer datenschutzrechtlichen Bestimmungen gerecht zu werden.
- Datenverschlüsselung: Die Notwendigkeit der Datenverschlüsselung führt zu einer zusätzlichen Komplexitätsstufe in einem bereits sehr komplexen Sachverhalt.
- Daten-Pseudonymisierung: Die technische Lösung hierfür ist in vielen Bereichen noch nicht ausgereift. Zusätzlich tritt bei dem Sonderfall der Offenlegung pseudonymisierter Daten an Dritte das Problem auf, dass die Daten ohne zusätzliche Informationen nicht mehr identifiziert werden können und somit die Offenlegung bei Anfrage erschwert wird.¹⁹

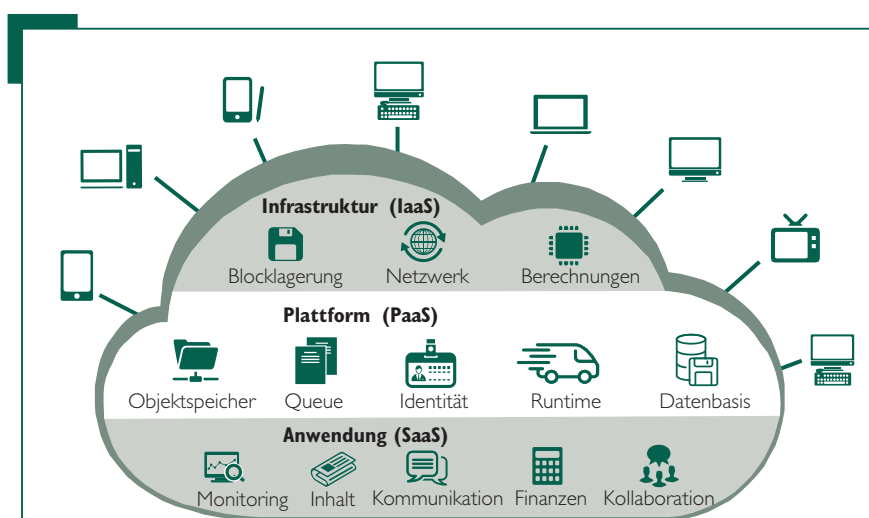


Abb. 1: Wesentliche Elemente der einzelnen Cloud-Kategorien

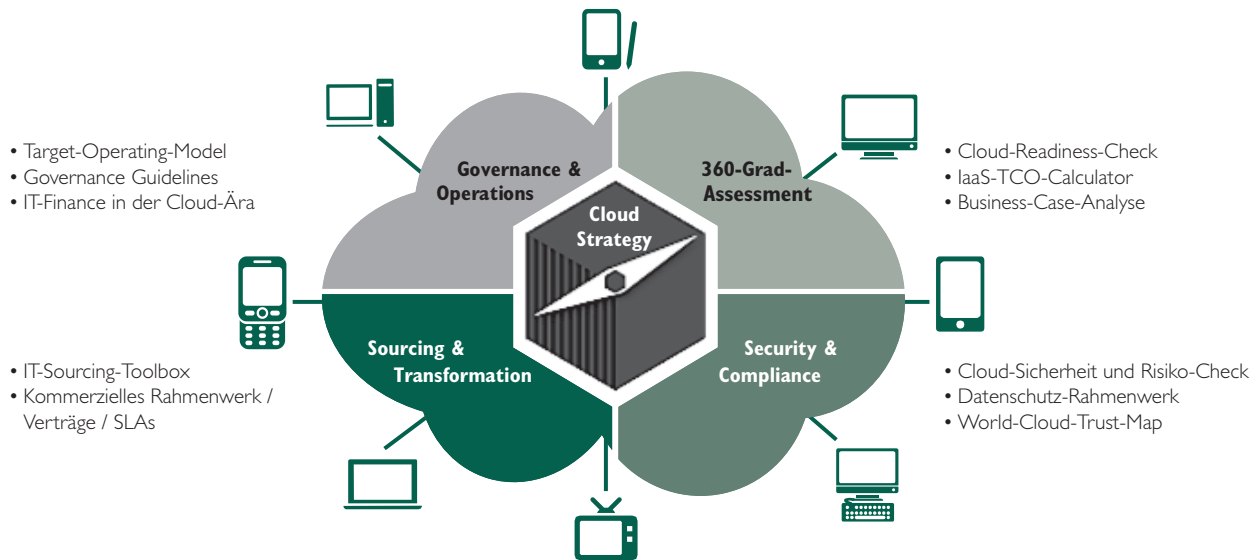


Abb. 2: Best Practice des Cloud-Navigator-Ansatzes

- Standort der Server / Ort der Datenverarbeitung / Zugriff: Es muss stets klar sein, in welchem Staat sich die Daten befinden, beziehungsweise von wo auf die Daten zugegriffen wird und ob in diesen Staaten ein vergleichbares Datenschutzniveau gewährleistet wird.
- FINMA Outsourcing Rundschreiben: Zu beachten ist auch der Aussagegehalt des FINMA Outsourcing Rundschreibens in Bezug auf die Zugriffsmöglichkeit notwendiger Daten bei der von Sanierung betroffenen Gesellschaften.²⁰
- Bring-your-own-key-Verschlüsselung: Dies ist derzeit bei den vielen Public-Cloud-Anbietern nicht ohne weiteres umsetzbar beziehungsweise vorgesehen.
- Kontrolle über Daten in der Cloud: Data-Profiling und -Mining durch den Public-Cloud-Anbieter bedarf unter Umständen eine dezidierte Einvernehmungserklärung der betroffenen Person.
- Aufbewahrungszeit: Einhaltung einer imitierten «Retention Period» der Daten in einer Public Cloud, nachdem der Vertrag mit dem Cloud-Anbieter gekündigt wurde.

Komplexität in der Public Cloud adressieren und so reduzieren

Im Ergebnis führt die immer weitreichendere und vielschichtiger werdende Regulierung zu neuen und vor allem komplexeren Herausforderungen. Um diesen gerecht zu werden, erhöhen sich die Anforderungen an die Konfiguration und Durchlässigkeit von Datensystemen dabei signifikant. Nicht zu vergessen sind hierbei auch die gesonderte Betrachtung und Adaption von Business-Continuity-Plänen und die Erstellung beziehungsweise Anpassung eines Konzeptes zur Wiedereingliederung der ausgelagerten Dienstleistung. Für Unternehmen, die sich für eine Cloud-Lösung entscheiden, geht eine Externalisierung der Privatsphäre einher. Deshalb wäre es sicherlich wünschenswert, wenn eine massgeschneiderte Vereinbarung mit dem Cloud-Anbieter getroffen werden könnte, welche den Anbieter zur Einhaltung sämtlicher relevanter aufsichts- und datenschutzrechtlicher Bestimmungen verpflichtet. In der Praxis ist dies aber recht schwierig zu bewerkstelligen. Betrachten wir nämlich Public-Cloud-Lösungen und hier insbesondere die zugrundeliegenden Verträge näher, wird schnell ersichtlich, dass deren Aufbau als «Multi-Tenant»-Service ge-

genüber massgeschneiderten Lösungen grundsätzlich den individuellen Kundenbedürfnissen weniger Rechnung tragen.²¹

Wer nun als Folge der Herausforderungen das Verharren in lokal verwalteten Lösungen mit multiplen Datensilos propagieren möchte, wird in dieser rückwärtsgewandten Sichtweise aber auch keine adäquate Lösung finden, um den regulatorischen und datenschutzrechtlichen Anforderungen zu entkommen. Da es sinniger Weise keinen Bestandschutz für Legacy-Systeme geben kann, werden auch diese fit für die neuen regulatorischen und datenschutzrechtlichen Anforderungen gemacht werden müssen. Hier wird es sich nach Erfahrung der Autoren erweisen, dass die fehlende Agilität dieser Systeme einen limitierenden Faktor darstellt, um mit den regulatorischen Entwicklungen mit vertretbarem Ressourceneinsatz Schritt halten zu können. Während manuelle Anpassungen in vielschichtigen Systemen sehr aufwändig sind, besteht zugleich die Gefahr, dass nicht alle Anforderungen im erforderlichen Mass umgesetzt werden können.²² Daher kann, sofern richtig aufgesetzt, der Umstieg in eine Public-Cloud-Umgebung eine wertvolle und sinnvolle Investition sein.

Zu meisternde Herausforderungen bei Public-Cloud-Computing

Eine Studie von Commvault²³ belegt, dass nur 12 Prozent von 177 international agierenden IT-Organisationen derzeit verstehen, wie die europäische Datenschutzgrundverordnung deren cloud-basierte Lösungen beeinflusst. Gartner²⁴ prognostiziert zudem, dass 95 Prozent aller Cloudsicherheitsfehler im Jahr 2020 durch die Kunden der Cloud selbst verursacht werden.

Da bei Cloud-Lösungen auch die Bearbeitung von personenbezogenen Daten ausserhalb des Europäischen Wirtschaftsraums (EWR) möglich ist, wird generell empfohlen, eine länderübergreifende Cloud-Strategie zu definieren, um die Adäquanzanforderungen und die lokalen datengesetzlichen Bestimmungen einzuhalten. Hier können externe Experten, die weitreichendes unabhängiges Know-how über die einzelnen Provider und über die Anforderungen der aktuellen Gesetzeslage haben, einen wertvollen Beitrag leisten. BearingPoint empfiehlt, die entsprechenden Aspekte systematisch anhand eines Regulatory Public-Cloud-Assessment (Cloud-Navigator-Ansatz) zu adressieren.

Regulatory Public-Cloud-Assessment: in the cloud or down to earth?

Um zu bestimmen, ob der regulatorische Aufwand gerechtfertigt ist, eine Public-Cloud-Lösung (entweder als mittel- oder langfristigen Ersatz für existierende Systeme oder als Ergänzung) zu adaptieren, müssen in einem ersten Schritt das Geschäftsmodell, die eigene Systemlandschaft ebenso wie die zu erwartenden Aufwände für ein derartiges Projekt analysiert werden. Hierfür bietet sich ein allumfassendes Assessment an, welches das Unternehmen frühzeitig auf datenschutzrechtliche und regulatorische Bestimmungen sensibilisiert und die Bemühungen einer potenziellen Cloud-Integration initial in die richtige Richtung lenkt. Eine erfolgserprobte Möglichkeit stellt der Cloud-Navigator-Ansatz dar, der eine übergeordnete Cloud-Strategie

vorsieht, die sich sowohl auf die Grundpfeiler Assessment, Security und Compliance, Sourcing und Transformation wie auch auf Governance und Operations stützt. Im Folgenden wird der Ablauf eines Public-Cloud-Assessments skizziert (Abbildung 2).

360-Grad-Assessment

Am Anfang eines jeden Cloud-Implementierungsprojekts sollte ein Cloud-Readiness-Check stattfinden, um den Status quo der Prozess- und Systemlandschaft zu durchleuchten und mögliche Anknüpfungspunkte für die Cloud-Lösung zu definieren. Dabei werden bereits Entscheidungskriterien für die Bewertung von potenziellen Lösungen sowie Services definiert und ein Reifegradmodell erstellt, das als Basis für das weitere Vorgehen fungiert. Im Rahmen dieser Analyse werden die Vor- und Nachteile einer Cloud-Implementierung auf das jeweilige Unternehmen ersichtlich.

Im Rahmen des 360-Grad-Assessments bietet sich eine IaaS-Total-Cost-of-Ownership-Analyse (TCO-Analyse) unter Berücksichtigung der IT-Strategie an, um die erfolgsrelevanten Unterschiede einer Public-Cloud- beziehungsweise einer On-Premise-Lösung zu definieren. Ergebnis ist ein Report, der die Kostenunterschiede der verschiedenen Lösungen ausweist. Dieser dient als Grundlage für eine Business-Case-Analyse. Dabei werden Risiko-, Nutzen- und Wirtschaftlichkeitsfaktoren strukturiert aufgearbeitet, um den Entscheidungsträgern eine fundierte Informationsbasis für oder gegen eine Cloud-Lösung bereitzustellen und ein realitätsgerechtes Bild der zu erwartenden Kosten geschaffen. Parallel werden im Rahmen des Assessments Kompatibilitätsprüfungen der einzelnen Systeme und möglicher Cloud-Architekturen forciert.

Security und Compliance

Das Assessment unterstützt im Rahmen der Cloud-Security- und Compliance-Phase eine frühzeitige Auseinandersetzung mit den regulatorischen Anforderungen. Neben der Analyse der World-

Cloud-Trust-Map, die die weltweite Datenschutzlage aufzeigt, kann anhand von Sicherheits-Checklisten der Europäischen Agentur für Netz- und Informationssicherheit²⁵ (ENISA) das Sicherheitsrisiko kategorisiert werden. Demnach können die jeweiligen Anwendungsfälle für eine Public Cloud frühzeitig identifiziert werden, die nötigen Ressourcen frühzeitig geplant und ein strukturierter Ablauf hin zur durchgängigen Compliance gewährleistet werden. Durch die Flexibilität der Lösung ist eine zeitnahe Definition flankierender Massnahmen zur Adaption länderspezifischer regulatorischer Anforderungen möglich.

Bewertung der Cloud-Angebote einzelner Anbieter

Ähnlich wie bei der Konfiguration eines neuen Fahrzeugs ist zunächst zu evaluieren, welche «Serienausstattung» von den verschiedenen Cloud-Anbietern in deren «out-of-the-box»-Angeboten enthalten ist. Nur so lässt sich abschätzen, welche regulatorischen Anforderungen bereits von diesen Angeboten abgedeckt sind und welche Anforderungen im Laufe der Vertragsgestaltung zu berücksichtigen sind beziehungsweise auf anderen Wegen erfüllt werden müssen. Diese «Gap-Analyse» mündet in einem Massnahmenplan, der die notwendigen Schritte aufzeigt, um regulatorische und datenschutzrechtliche Compliance zu erzielen.

Im Rahmen dieses Assessments inklusive Kosten-Nutzenanalyse und Cloud-Provider-Analyse wird aufgezeigt, welche Umsetzungsstrategie die Anforderungen der vorhandenen Datenstrukturen erfüllt und wie ein Umsetzungsplan zu erfolgen hat.

Governance und Organisation

Es liegt in der Natur der Sache, dass der Massnahmeplan zumindest mit – unter vertretbarem Aufwand realisierbaren – technischen Möglichkeiten keine vollständige regulatorische und datenschutzrechtliche Compliance erreichen können wird. Sowohl auf Ebene «Plattform» als auch auf Ebene «Anwendung»

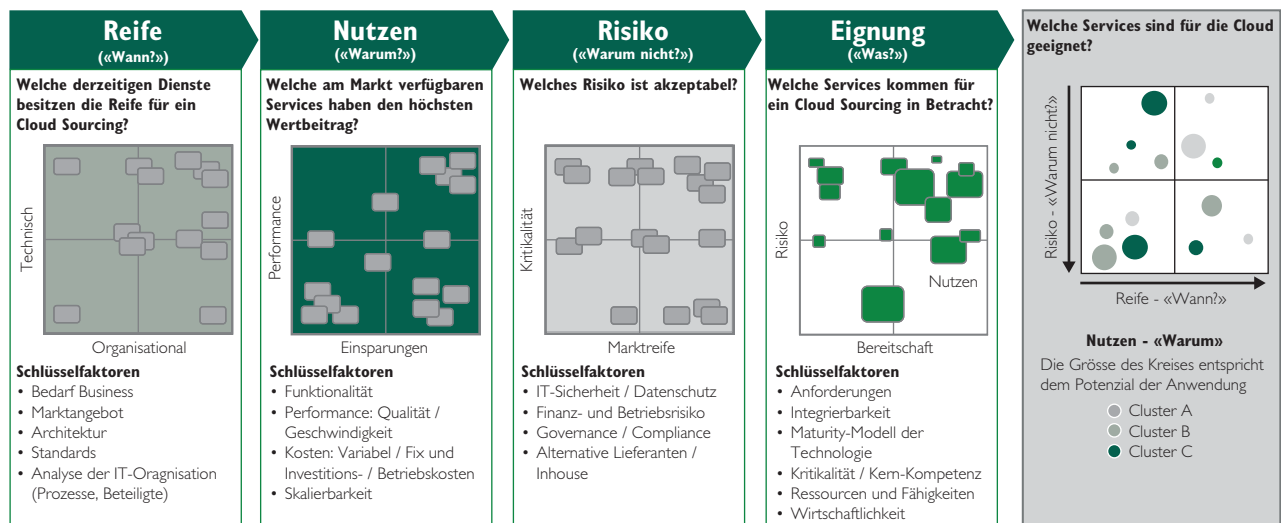


Abb. 3: Reifegradanalyse im Rahmen des Public-Cloud-Assessments

wird in der Praxis nicht jeder einzelne Anwendungsfall perfekt adressiert werden können. Um diesem Umstand Rechnung zu tragen, ist darüber hinaus eine Governancestruktur zu entwickeln, die die noch nicht hinreichend adressierten Anforderungen bedient. Mit standardisierten Genehmigungszyklen für Sonderfälle, Kontroll- und Überwachungsmechanismen sowie Eskalationsmöglichkeiten kann somit letzten Endes vermieden werden, dass zwingende regulatorische Vorschriften verletzt werden.

Als Ergebnis des Regulatory Public-Cloud-Assessments lässt sich anschliessend eine Reifegradanalyse erstellen, anhand deren abgeleitet werden kann, welche einzelnen Anwendungsfälle für eine Public-Cloud-Lösung aus regulatorischer Sicht überhaupt in Frage kommen (Abbildung 3).

Fazit

Public-Cloud-Transformationsprogramme haben vielschichtige Herausforderungen zu bewältigen, bis datenschutzrechtliche und regulatorische Anforderungen hinreichend abgedeckt sind. Zur Prüfung der Cloud Readiness, bietet sich ein Regulatory-Public-Cloud-Assessment an. In einem ersten Schritt sind die relevanten Anforderungen zu identifizieren, da-

mit diese entsprechend adressiert werden können. Die zur Umsetzung erforderlichen flankierenden Massnahmen sind anschliessend aus einem Abgleich zwischen dem Angebot des Public-Cloud-Anbieters und den regulatorischen, datenschutzrechtlichen Vorgaben zu entwickeln und im Nachgang entsprechend zu implementieren. Korrekt aufgesetzt kann ein Public-Cloud-Programm als Accelerator dienen, um die Umsetzung datenschutzrechtlicher Anforderungen anzugehen. Andererseits versprechen Public-Cloud-Programme individuelle Quick-Wins entlang der Operationalisierung von Anwendungsfällen ebenso wie auch eine Weichenstellung für die langfristige Effizienzsteigerung neuer datenbasierter Geschäftsmodelle in der Versicherungsindustrie.

Anmerkungen

- 1 Siehe: <https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/> (Zuletzt abgerufen: 10.04.2018).
- 2 Zur Information: Laut Berechnung befinden sich auf der Erde ca. 5 Trilliarden (1 Trilliarde = 1021) Sandkörner: Bei einem prognostizierten Datenvolumen von 163 Zettabyte entspricht die Byteanzahl mehr als ein 32-faches der geschätzten Sandkornanzahl der Erde; siehe: Marshall, Jason (2011): Why Math isn't an Awful Nerd, ebook. Oder online unter: <https://goo.gl/NGWby3> (Zuletzt abgerufen: 10.04.2018).
- 3 Siehe Berger, D.; Sängler, U. und Schnider, J.: «Wachstum durch neue Wege in der Kundenbindung für Krankenversicherer», in: Institut für Versicherungswirtschaft der Universität St. Gallen (Hrsg.), I-VW Management-Information – St. Galler Trendmonitor für Risiko- und Finanzmärkte. I / 2017, pp.17–19.
- 4 Moor, C.: CSS Blog – Bewegung ist wichtig. Wie viel Sport ist gesund?, online unter: <https://blog.css.ch/de/bewegung/tipps-de-bewegung/bewegung-ist-wichtig/> (Zuletzt abgerufen: 23.03.2018). Oder: Gesundheitskonto CSS, online unter: <https://www.css.ch/de/home/privatpersonen/krankenkasse/zusatzversicherung/gesundheitskonto.html#gesundheitskonto> (Zuletzt abgerufen: 03.04.2018).
- 5 Lamy, L. (2014): IDC Buyer Case Study – Connected Cars: How Jaguar Land Rover Works with BearingPoint to Benefit Drivers, online unter: https://www.bearingpoint.com/files/IDC_buyer_case_study-Connected_cars-Jaguar_Land_Rover_BearingPoint-1.pdf&download=0&itemId=5158 (Zuletzt abgerufen: 26.03.2018).
- 6 Heidrich, J.; Wegener, C. (2017). Betrieblicher Datenschutz (2. Auflage), Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.) mit der Feststellung, dass eine einheitliche Definition des Cloud Computing bisher weder in juristischer noch technischer Hinsicht existiere.
- 7 Die wichtigsten Vorteile von SaaS aus Sicht der teilnehmenden Unternehmen sind niedrigere Gesamtkosten und vereinfachte Versionspflege, siehe: Weidmann, Renner, Rex, Cloud Computing in der Versicherungsbranche – IT Trends im Internet der Dienste aus Sicht von Anwendern und Anbietern (2010), S. 79, online unter <http://wiki.iao.fraunhofer.de/images/studies/cloud-computing-in-der-versicherungsbranche.pdf> (zuletzt abgerufen 07.05.2018).
- 8 Der grösste Vorteil ist jedoch vermutlich, dass Unternehmen keine hohe Investition für teure IT-Infrastruktur tätigen müssen, sondern sich direkt an bereits etablierte Lösungen halten können. Auch die Vielzahl von Cloud-Anwendungen ermöglicht es, flexibel auf neue Geschäftsprozesse und Möglichkeiten zu reagieren; siehe: Tezel, Cloud Computing: SaaS, PaaS & IaaS einfach erklärt, ZD-Aktuell 2016, 05026, beck-online.
- 9 Weidmann, R. R., ebenda, S. 76.
- 10 Als Vorreiter sind hier beispielsweise Uber und Amazon zu nennen, wobei Finanzdienstleister, wie Banken und Versicherer, die in einem klassischen Produktpipeline-basierten Geschäftsmodell ver-

bleiben, dem Gedanken der Plattformökonomie im Grundsatz widersprechen und mit der Empfehlung, diesbezüglich einen Umdenkprozess zu starten, wohl gut beraten wären.

- 11 s. Art. 6 DSGVO und Erwägungsgrund Artikel 103, Artikel 104 und Artikel 45 Abs. 1 EU DS-GVO.
- 12 Über ein hinreichendes Datenschutzniveau verfügen aus Sicht der EU Kommission ausserhalb der EU nur wenige andere Staaten, wie z.B. Andorra, Argentinien, Australien, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Kanada, Israel, Schweiz oder Uruguay (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_de#relatedlinks).
- 13 Europäische Kommission (2016): EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, online unter: http://europa.eu/rapid/press-release_IP-16-216_en.htm (Zuletzt abgerufen: 23.03.2018).
- 14 Kritisch hierzu und teilweise abweichend: Mitteilung der Kommission an das Europäische Parlament und den Rat zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der RL 95/46/EG nach dem Urteil des Gerichtshofs in der Rs. EUGH Aktenzeichen C-362/14 (Schrems), Brüssel, 6.11.2015, COM(2015) 566 final.
- 15 Rat der Europäischen Union (2016): General Data Protection Regulation, online unter: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf> (zuletzt abgerufen: 23.03.2018)
- 16 Personenbezogene Daten sind alle Daten, die auf eine bestimmte Person schliessen lassen. Dazu zählen neben dem Namen, Identifikationsnummern, Foto, Ort und E-Mail-Adresse auch Online-Kennung, IP-Adressen und Kombinationen aus wirtschaftlichen, genetischen, physikalischen, kulturellen, medizinischen oder sozialen Informationen.
- 17 Roßnagel, in: ders. (Hrsg.), Europäische Datenschutz-Grundverordnung, 2017, S. 67 ff
- 18 Art. 4 Abs. 2 Bst. j i.V.m. Art. 5 Abs. 2 Versicherungsaufsichtsgesetz
- 19 Siehe <https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung> (Zuletzt abgerufen: 27.04.18).
- 20 FINMA-RS 18/3 «Outsourcing – Banken und Versicherer» Auslagerungen bei Banken und Versicherungsunternehmen (21. September 2017) «Die Sanierbarkeit bzw. Abwickelbarkeit des Unternehmens in der Schweiz muss gewährleistet sein. Der Zugriff auf die dafür notwendigen Informationen muss jederzeit in der Schweiz möglich sein.» <https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finmars-2018-03.pdf?la=de> (Zuletzt abgerufen: 27.04.18).
- 21 So statuiert etwa ein grosser Anbieter hinsichtlich der Adaption von Security Policies seinen Kunden: «As multitenant services, ... and ... are unable to agree to comply with any particular company's security policy.»
- 22 Die Erfahrung der Autoren ist, dass gerade in der Versicherungsindustrie das Alter der Bestandssysteme oftmals denen der Lebensversicherungsverträge, die sie verwalten, in nichts nachstehen.
- 23 Siehe: <https://www.computerworlduk.com/cloud-computing/predicting-biggest-cloud-trends-in-2018-3669252/> (Zuletzt abgerufen am: 28.03.2018).
- 24 Siehe: <https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/> (Zuletzt abgerufen am: 10.04.2018).
- 25 Siehe https://europa.eu/european-union/about-eu/agencies/enisa_de (Zuletzt abgerufen: 10.05.18).

Gezieltes Engagement

BearingPoint bietet Management- und Technologieberatung, die Strategien mit neuen technischen Möglichkeiten verknüpft. Wir entwickeln individuelle Lösungen auf persönlicher Basis. Unternehmen und Organisationen profitieren von messbaren Ergebnissen, wenn sie mit uns zusammenarbeiten.

www.bearingpoint.com



BearingPoint®