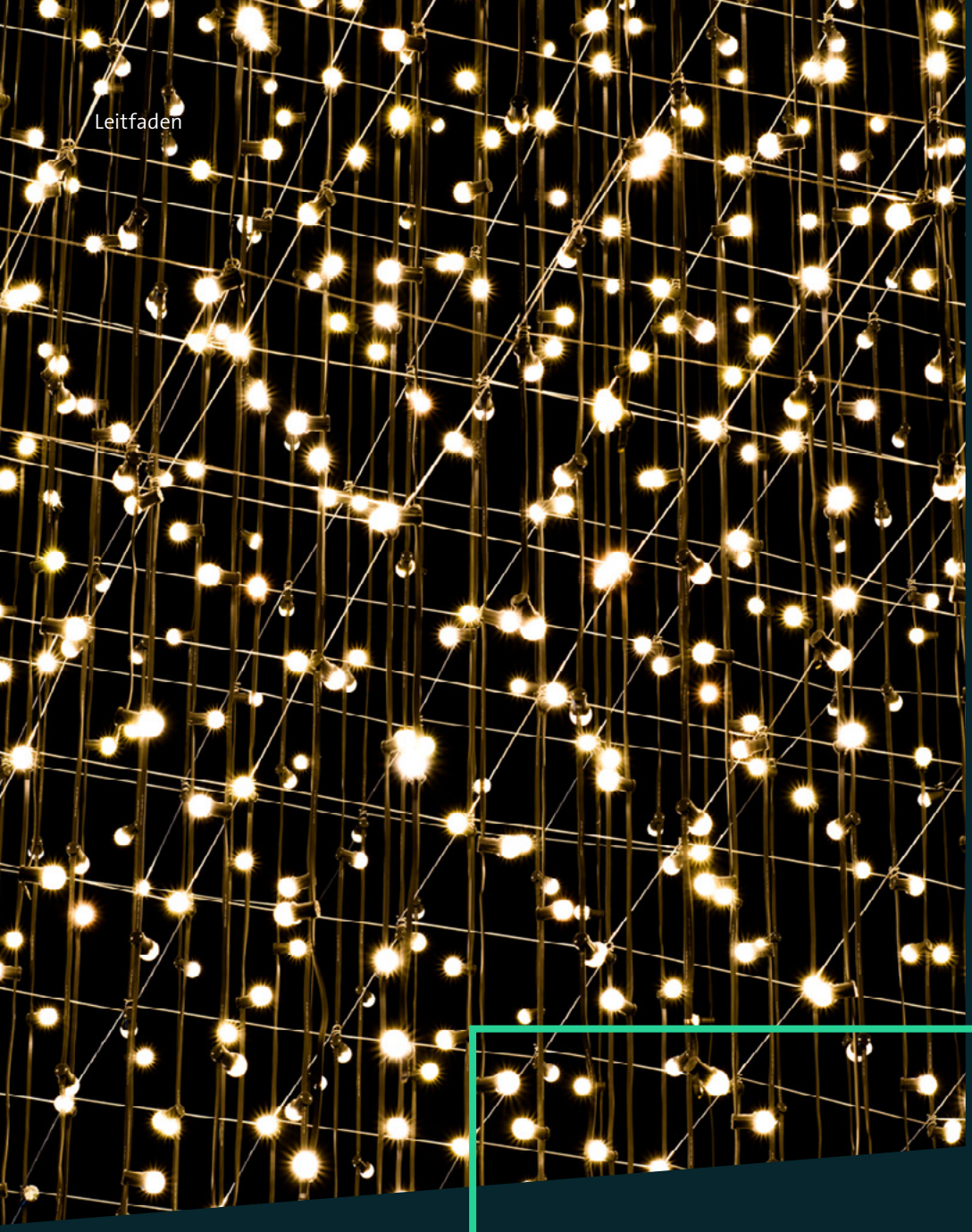

Leitfaden

bitkom

Der Weg in die Cloud im Versicherungsökosystem

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Gustav Spät | Trainee Digitale Transformation
T 030 27576-137 | g.spaet@bitkom.org

Kevin Hackl | Bereichsleiter Digital Banking & Financial Services
T 030 27576-109 | k.hackl@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digital Insurance & InsurTech

Autorinnen und Autoren
Martin Diehl (NTT Data) | Dr. Klaus Driever (Allianz) | Dr. Wolff Graulich (Eucon) | Philipp Koch (Senacor) | Dr. Philipp Rietsch (Senacor) | Axel Saß (Red Hat) | Armin Schübel (Capgemini) | Christoph Seidl (Senacor) | Irina Toncheva-Germanova (Capgemini) | Fabian Warthenpfuhl (NTT Data) | Lars Willrich (Senacor)

Layout
Lea Joisten

Titelbild
© Peter Wey – stocksy.com

Inhalt

Cloud-Technologien sind heutzutage selbst im Markt der hoch regulierten Versicherungsunternehmen längst angekommen. Auch wenn sich die einstige Hoffnung, dass Cloud-Technologien über eine dynamische Skalierung eine Reduzierung von betrieblichen Kosten erreichen können, nur bedingt bewahrheitet hat, sind heute ganz andere Vorteile Treiber für die Migration in die Cloud.

Ein Kernpunkt ist hier, die hohe Agilität in der modernen Softwareentwicklung auf die Infrastruktur übertragen zu können. Die Dynamik und die nahezu endlose Möglichkeit zur Skalierung hilft dabei, transparent, schnell und flexibel auf die Anforderungen von Kundinnen und Kunden reagieren zu können. Änderungen an der Infrastruktur, welche in klassischen Betriebsorganisationen meist mehrere Wochen dauern, lassen sich mittlerweile über integrierte Development, Security und Operations (DevSecOps) Teams schnell, nachvollziehbar und sicher innerhalb von kürzester Zeit durchführen. Dies ermöglicht nicht nur, die Time-to-Market drastisch zu reduzieren, sondern fördert die Innovationskraft des Unternehmens.

Zudem bieten global agierende Hyperscaler sehr einfache Möglichkeiten, eine hohe Ausfallsicherheit, georedundante Verteilung oder sogar die Erschließung von ausländischen Märkten mit einer jeweils regionalen Infrastruktur und Datenhaltung zu gewährleisten.

Einen weiteren Kernpunkt einer Cloud-affinen IT-Organisation offenbart auch der Blick auf die sogenannten Cloud-Assets. Hier geht es nicht nur um die Möglichkeit, betriebsrelevante Technologien und Produkte durch sogenannte Managed Services zu ersetzen, sondern vielmehr um die Möglichkeit, über sogenannte Software as a Service (SaaS)-Produkte das eigene Portfolio um Mehrwert schaffende Dienste zu erweitern. Im Versicherungsbereich kann dies beispielsweise die Anbindung einer speziellen Schaden-Plattform oder die Auslagerung von ganzen Teil-Prozessen an ein InsurTech-Unternehmen sein. So kann sich die Organisation auf ihre Kernkompetenz und die damit verbundenen Stärken fokussieren.

Doch gerade im hoch regulierten Versicherungsbereich herrscht aufgrund der sehr hohen Anforderungen an Compliance und Security (immer noch) eine große Unsicherheit, ob eine Transformation in die Cloud möglich und vor allem rechtssicher ist. Hier gilt es zu klären, wie die Vorgaben zu den Versicherungsaufsichtsrechtlichen Anforderungen an die IT (VAIT) der Bafin und der DSGVO erfüllt werden können.

Die Vergangenheit hat gezeigt, dass viele Unternehmen, welche ohne eine vollumfängliche Strategie erste Schritte in Richtung Cloud-Nutzung gegangen sind, in ihrer Migration gescheitert bzw. stecken geblieben sind. Grund ist hier oft fehlendes Wissen und Verständnis, welche Möglichkeiten die Cloud bietet und welche Grundlagen geschaffen werden sollten, um die Cloud effizient zu nutzen. Vor allem ist zu bedenken, dass eine echte Cloud Migration eine ganzheitliche Änderung der betroffenen Unternehmen und im speziellen der IT-Organisation erfordert. Hier ist die technische Herausforderung oft kleiner als die organisatorische. Alte Denkmuster und »althergebrachte« IT-Organisationen, beides keine Seltenheit im Insurance-Bereich, tragen hierzu ihren Teil bei.

Entscheidend ist außerdem die Wahl des richtigen Business Case für den Treiber der Cloud-Transformation. Ist dieser richtig gewählt, zeigt er schnell den Nutzen für die Migration und überzeugt die Zweifler. Ist er falsch gewählt, kann das schnell ins Gegenteil umschlagen.

Nicht zuletzt hat auch die Außendarstellung der Cloud-Anbieter, die wenig auf Herausforderungen und Probleme beim Gang in die Cloud sowie die nötige digitale Transformation hinweisen, dazu beigetragen, dass in vielen Unternehmen immer noch Zurückhaltung herrscht, wie die Cloud für den eigenen Markt am besten genutzt werden kann.

Trotz dieser Herausforderungen zeigt sich in Anbetracht der Vorteile einer Cloud-Nutzung unserer Meinung nach, dass der Verzicht auf eine Cloud-Transformation einen langfristigen Wettbewerbsnachteil mit sich bringen würde. Damit erübrigt sich für uns die Frage, »ob« man als Versicherungsunternehmen die Cloud nutzen sollte und wir stellen uns im Folgenden der Herausforderung, das »wie« zu beschreiben. Daher widmet sich dieses Papier insbesondere auch den Voraussetzungen, die nötig sind, um die genannten Vorteile nutzen zu können und den Veränderungen in der Wertschöpfung. In Kapitel 1 werden wir – eher fachorientiert aber allgemein aufschlussreich – Data, Compliance und Security betrachten und wie Technologie hier unterstützt. Transformation von IT und Organisation wird in Kapitel 2 genauer beschrieben, bevor in Kapitel 3 der Blick auf Governance und optimale Wertschöpfung mit neuen und alten Partnern gerichtet wird. Kapitel 4 schließt das Papier mit einem Fazit ab.

1 Compliance, Data, Security: Technologie hilft bei den großen Cloud-Fragestellungen

Im Zuge der Digitalisierung setzen immer mehr Versicherungen auf Cloud-Computing. Allerdings zögern, wie oben beschrieben, immer noch viele Unternehmen, eine umfassende Cloud-Transformation anzugehen. Haupthindernisse sind dabei unter anderem die große Anzahl und die Komplexität der Anforderungen, die deutsche und europäische Behörden und Institutionen an die Cloud-Nutzung von Versicherungen stellen. Im Wesentlichen spielt die konkrete Applikationsklassifizierung bzw. die genaue Untersuchung von Zweck und Ziel der auszulagernden Applikation und der zugehörigen Daten eine entscheidende Rolle bei der Bestimmung der konkreten Regularien, die die Versicherungen bei der Cloud-Nutzung berücksichtigen müssen. Bei der Migration von Applikationen ohne Relevanz für das Versicherungsgeschäft sind typischerweise weniger technische Maßnahmen zur Cloud-Risikomitigierung erforderlich als bei Applikationen mit Relevanz für das Versicherungsgeschäft. Im Folgenden werden wir die geltenden Cloud-Compliance-Regelungen und deren mögliche Risikomitigierungsmaßnahmen mit verstärktem Fokus auf die Technik betrachten.

1.1 Cloud-Compliance-Anforderungen an Versicherungsunternehmen

Seit dem Pandemiebeginn Anfang 2020 wurden verstärkt Regularien auf den Weg gebracht, die direkte Auswirkungen auf die Herangehensweise der Cloud-Nutzung in Versicherungsunternehmen haben. Versicherungen müssen sich einen Überblick über die geltenden Cloud-Compliance-Anforderungen verschaffen, bevor sie mit konkreten Umsetzungsschritten für eine Cloud-Migration starten. Je nach Herkunft der Cloud-Compliance-Anforderungen können diese in drei Kategorien eingeteilt werden – aufsichtsrechtliche Anforderungen, Datenschutz- und Sicherheitsanforderungen, sowie gewerbliche bzw. steuerrechtliche Anforderungen.

- Zu den aufsichtsrechtlichen Anforderungen gehören bekannte Auslagerungsvorschriften wie die MaGo und die VAIT. Hierunter fallen auch die Cloud-spezifischen Orientierungshilfen der Bafin und der EIOPA sowie – zukünftig – auch der Digital Operational Resilience Act (DORA).

- In der zweiten Kategorie werden Datenschutz- und Sicherheitsaspekte wie DSGVO, C5 (BSI), IT-Sicherheitsgesetz und StGB eingeordnet. Bei Auslagerung von personenbezogenen Daten ist die DSGVO besonders relevant. Die Datenschutz- und Sicherheitsaspekte werden in den nächsten Abschnitten detaillierter dargestellt.
- In die dritte Kategorie fallen die gewerblichen und steuerlichen Compliance Anforderungen. Diese gelten für alle Versicherungsunternehmen, die einer Wirtschaftsprüfung unterliegen, und werden insbesondere dann relevant, wenn rechnungslegungsrelevante Daten bzw. für die Solvenzbilanz relevante Daten in die Cloud ausgelagert oder dort erzeugt werden. In diesem Fall stellen unter anderem Jahresabschlussprüfer und Gesetzgeber im HGB ihrerseits Anforderungen an die Cloud-Auslagerung. Ein Beispiel ist die Datenverschlüsselung mit der Bring Your Own Key (BYOK)-Methode, die von IDW RS FAIT 5 verlangt wird und auf die wir später genauer eingehen werden.

Die Compliance-Anforderungen enthalten teilweise Überschneidungen hinsichtlich ihrer Vorgaben zur Cloud-Nutzung. Es empfiehlt sich daher, von Anfang an ein zentrales Cloud-Compliance-Framework zu definieren, das die Vorgaben aus den unterschiedlichen Compliance-Anforderungen sammelt. So wird Transparenz gegenüber aktuellem und zukünftigem Stand der Cloud-Compliance erreicht. Darauf aufbauend können auch klare Verantwortlichkeiten und konkrete Umsetzungsschritte in Bezug auf die aus den Vorschriften abgeleiteten risikomitigierenden Maßnahmen definiert werden. Die häufigsten Maßnahmen zur Risikomitigierung bei der Cloud-Nutzung können als vertraglich, organisatorisch und technisch kategorisiert werden.

- Zu den vertraglichen Maßnahmen zählen umfangreiche Anforderungen an den Cloud-Anbieter inkl. Regelungen bzgl. möglicher Weiterverlagerungspartner, umfassende Kündigungsrechte etc.
- Die organisatorischen Maßnahmen beinhalten die Durchführung einer Due-Diligence-Prüfung des Cloud-Anbieters, die Risikobewertung des Cloud-Vorhabens, die Sicherstellung der Sicherheit von Daten und Systemen, Erstellung von Datenschutzfolgeabschätzungen, sowie die Erstellung solider Exit-Strategien und Governance Mechanismen. Der genaue Umfang der umzusetzenden risikomitigierenden Maßnahmen wird durch die Risikobewertung bestimmt. Ein zentraler Punkt der Risikobewertung ist die Analyse auszulagernder Daten hinsichtlich Wesentlichkeit und Kritikalität. Generell gilt: Je höher die Kritikalität der Daten, desto umfangreicher müssen die Risikomitigierungsmaßnahmen zum Cloud-Vorhaben sein. Mögliche Optionen stellen wir im nächsten Abschnitt vor.

- Für die technischen Maßnahmen bieten die Cloud-Anbieter Frameworks und Tools für Compliance und Security Aspekte, die die Umsetzung der Risikomitigierungsmaßnahmen unterstützen. Mithilfe dieser Technologien und Werkzeuge lässt sich die Implementierung eines zentralen Cloud-Compliance-Frameworks systematisch in größtenteils automatisierten Schritten und Prozessen abbilden. Damit haben die Versicherungsunternehmen eine vollständige Übersicht aller aktuellen oder geplanten technischen Maßnahmen hinsichtlich Cloud-Compliance und Security zur Hand. Zusätzlich können sie bei Anfragen der Aufsicht mit wenig Aufwand ausgewertet werden. Beispiele für Automatisierung im Bereich Compliance und Security stellen Compliance-As-Code-Produkte dar, die das Durchführen von Compliance und Security Tests auch in die Automatisierung integrieren und die Einhaltung von Sicherheitsrichtlinien automatisch sicherstellen. Daraus resultierend werden nicht nur enorme Zeitersparnisse, sondern auch schnelle Reaktionszeiten bei potentiellen Angriffen erreicht, da die Prüfung nach Compliance- und Sicherheitslücken regelmäßig und automatisiert erfolgt. Die (teil-)automatisierte und standardisierte Dokumentation all dieser Tätigkeiten ist ein weiterer wichtiger Faktor gegenüber aufsichtsrechtlichen Verpflichtungen.

1.2 Daten sicher in die Cloud migrieren

Das Schützen von Unternehmensdaten in der Cloud ist ein zentrales Thema, das spätestens seit 2018 durch den US »CLOUD Act« und seit 2021 auch durch das Schrems II Urteil erneut im Fokus steht. Alle amerikanischen Unternehmen (u. a. die Hyperscaler Amazon, Microsoft und Google) sind dazu verpflichtet, US-Behörden auf Nachfrage Zugriff auf gespeicherte Daten zu gewährleisten, auch wenn die Speicherung außerhalb der USA erfolgt. Als wirksamer Ansatz zur Risikomitigierung hat sich die Datenverschlüsselung bewährt, da sie gewährleistet, dass im Falle eines Datendiebstahls oder einer Datenweitergabe an Geheimdienste nur unlesbare und damit unbrauchbare Informationen die Cloud-Umgebung verlassen.
Aus Sicht der IT-Sicherheit sind folgende drei Szenarien gemeint:

- Datenverschlüsselung in Übertragung (Data in Transit)
- Datenverschlüsselung in Bearbeitung (Data in Use)
- Datenverschlüsselung im Ruhezustand (Data at Rest)

In Bezug auf Data in Use und Data at Rest sind die gängigsten Datenverschlüsselungsmethoden für die Cloud (Data in Transit im nächsten Abschnitt):

- Bring Your Own Key (BYOK)
- Bring Your Own Encryption (BYOE)
- Hold Your Own Key (HYOK)

Obwohl es keine »One Size Fits All«-Lösung gibt, welche die Verschlüsselungsproblematik vollständig löst, gilt die BYOK-Methode als die führende Lösung in diesem Bereich. Bei dieser Methode führt der Cloud-Anbieter die Ver- und Entschlüsselung der Daten durch. Die Kundinnen und Kunden erzeugen und verwalten die Schlüssel eigenständig. Dieser Ansatz erfüllt somit insbesondere auch die Anforderung nach einer eigenen Schlüsselverwaltung gemäß des IDW RS FAIT 5. Die BYOE-Methode sieht vor, dass der Cloud-Kunde neben den selbst generierten Schlüsseln auch eigene kryptographische Algorithmen zur Datenverschlüsselung verwendet und dies nicht dem Cloud-Anbieter überlässt. So ist es bei BYOE, im Gegensatz zu BYOK, dem Cloud-Anbieter nicht möglich, einen Masterschlüssel zu generieren, da der Cloud-Anbieter keine Kenntnis über den eingesetzten kryptographischen Algorithmus besitzt. Die dritte Methode, HYOK, beschreibt ein Verschlüsselungsverfahren, bei dem Daten bereits vor der Übertragung in die Cloud verschlüsselt werden. Allerdings gehen viele der innovativen Vorteile der Cloud-Technologien mit diesem Verschlüsselungsansatz verloren, da die Daten in der Cloud nicht direkt bearbeitet werden können. Aus diesem Grund ist HYOK generell eher für eingeschränkte Anwendungsszenarien wie z. B. Speicherung und Archivierung von hochsensiblen Daten und Dokumenten empfohlen. Speziell beim Betrieb von Anwendungen in einer Cloud-Umgebung stellt sich die Frage, wie verhindert werden kann, dass unternehmensfremde Personen, zum Beispiel Administratoren der Cloud-Anbieter, auf Anwendungen und deren Daten zugreifen. Es gibt verschiedene Möglichkeiten diesen Zugriff zu verhindern. Den Anfang macht die prozessorbasierte Verschlüsselung in Form einer Secure Enclave. Dabei wird durch Mechanismen der CPU der Zugang zu Informationen verhindert bzw. diese verschlüsselt. Die Methode begrenzt aber nicht die Kommunikation in einer verteilten Applikation – dafür muss zusätzlich die Interaktion der verschiedenen Anwendungsteile abgesichert werden. Um dieses Problem zu lösen, werden aktuell Trusted Execution Environments (TEE) entwickelt. Hierbei werden gesamte Cluster / einzelne Nodes (Secure VM / Cluster) verschlüsselt und somit auch der Datenverkehr innerhalb eines Clusters abgeschottet, ohne die Notwendigkeit zu schaffen, jede einzelne Interaktion zu verschlüsseln. Erst wenn eine Information aus dem Cluster heraus an einen anderen Cluster / Service geschickt wird, muss explizit für eine Verschlüsselung gesorgt werden.

1.3 Sicherheit in der Cloud gewährleisten

Gerade in der Zeit der Pandemie und dem damit verbundenen Schub der Digitalisierung stehen die Themen rund um Sicherheit im Fokus. Die Einbeziehung von Cloud-Diensten stellt Unternehmen hier vor neue Herausforderungen. Hierbei geht es um Absicherung von Zugriffen, einem Rechtekonzept und der Ausführung von Business-kritischem Anwendungscode in einer externen Umgebung. Die Anzahl der Angriffe auf aus dem Internet erreichbare Dienste steigt ebenfalls, so dass auch hier neue Risiken entstehen, die angegangen werden müssen.
Es lassen sich drei Teilbereiche erkennen:

- Absicherung des Netzwerkverkehrs (Data in Transit)
- Absicherung und Logging der Zugriffsrechte
- Beseitigung von Sicherheitslücken und der damit verbundene Deploymentprozess von neuen Applikationen und Applikationsteilen in eine oder mehrere Umgebungen von Cloud-Anbietern.

Für die Absicherung des gesamten Verkehrs zwischen den Applikationen / Teilen der Applikation sollte TLS / SSL genutzt werden. Hier müssen die Applikationen daraufhin untersucht werden, ob eine Kommunikation stattfindet und falls ja, welche Protokolle derzeit genutzt werden bzw. gibt es eine andere Möglichkeit außer TLS sicher zu stellen, dass es zu keiner sogenannten »Man In The Middle« Attacke kommt?

Für die Absicherung der Zugriffsrechte auf die Umgebung und die darin enthaltenen Applikationen sind entsprechende Fragen an die Cloud-Anbieter zu stellen, um sicher zu stellen, dass der Zugriff durch Unberechtigte ausgeschlossen ist. Wie auch bei Inhouse-Umgebungen sollte dabei ebenfalls nach Verfahren gefragt werden, die Administrator-spezifische Prozesse beinhalten. Zum Beispiel: Was passiert, wenn ein Cloud-Service-Provider-Administrator das Unternehmen verlässt? Wie werden Auditlogs vorgehalten? Was wird auditiert? Woher kommen die Rechte in den hauseigenen Applikationen und den unternehmensinternen Administratoren? Wie kann die aufsichtsrechtliche Anforderung (VAIT Teilziffer 36) nach einer Zuordnung von technischen Benutzern zu natürlichen Personen sichergestellt werden? Aus einem unternehmensinternen Directory? Und wie werden diese Informationen in der Cloud bereitgestellt?

Letztlich ist dann der gesamte Bereich des Patchings der Applikationen bei einer Nutzung von Cloud-Diensten wichtig. Dabei sind diese Herausforderungen vor allem in Bezug auf die verwendete zu Grunde liegende Technik zu verstehen. Bei Verwendung von virtuellen Maschinen ist die Unterscheidung zwischen Cloud und On Premise überschaubar. Auch hier muss ein entsprechendes Tool jede Maschine durchsuchen und auf Schwachstellen untersuchen.

Allerdings gibt es bei der Verwendung von Cloud-typischen Container-Technologien Erweiterungen, die durch Frameworks und erweiterte Tools gelöst werden können. Die Anzahl der Container Images wird im Schnitt erheblich höher sein als die Anzahl bei virtuellen Instanzen. Hierbei werden die verschiedenen Versionen in einer Registry vorgehalten und zum Ausführungszeitpunkt dort geladen und genutzt. Aufgrund dieser hohen Anzahl ist es sehr aufwendig bei Bekanntgabe von Sicherheitslücken alle Images daraufhin zu untersuchen, welches Image mit welcher Version bereitgestellt wurde und ob ein Patching notwendig ist. Hier gibt es Tools, die im Rahmen des CI / CD-Prozesses die Einhaltung von Unternehmensrichtlinien durchsetzen bzw. Tools, die sich in die Registry einbinden und dort die hinterlegten Images kontinuierlich untersuchen und Hinweise geben, in welchem Zustand sich ein Image befindet.

Eine weitere Herausforderung ist die Suche nach Sicherheitslücken in eingebundenen Bibliotheken von virtuellen Instanzen und Containern. Hier beginnt sich ein Standard zu entwickeln, bei dem die Hersteller von Software Produkten mit Hilfe einer Software ein Inhaltsverzeichnis von verwendeten Bibliotheken bereitstellen, so dass das Finden von betroffenen Klassen erheblich einfacher wird.

Bei der Einbindung von SaaS können viele dieser Themen im Rahmen der Supply Chain Security an die Anbieter abgegeben werden. Fragen wie »Wer darf bei dem Service was tun?« und »Wer hat was gemacht?« sind von dem Service-Anbieter zu beantworten. Mitführen von Auditlogs und Security-patching-Logs sind dementsprechend beizubringen.

2 Roadmap – Transformation von IT und Organisation in einem meist hybriden Cloud-Betrieb

Die Art der Transformation und damit auch die Gestalt der Roadmap ist primär von den Zielen abhängig, die wir mit den strategischen Zielen der Cloudnutzung verbinden. Verschiedene typische Ziele, die bei Versicherungsunternehmen mit dem Wunsch, »in die Cloud zu gehen«, verknüpft sind, erfordern unterschiedliche Ausprägungen von Transformationen und Roadmaps. Wir schauen uns drei exemplarische Ziele an, die zur Cloud-Nutzung motivieren könnten.

- Entlastung der Betriebsorganisation: Dieses Ziel wird häufig mit der Nutzung von SaaS-Angeboten verknüpft. Standardsoftware wird im SaaS-Modus in der Hoffnung eingeführt, dass die wesentlichen betrieblichen Belastungen beim Hersteller und nicht in der eigenen Betriebsorganisation liegen.
- Geringere Kosten, höhere Transparenz, Leistung und Verfügbarkeit: Bei der Verfolgung von einem oder mehrerer dieser Aspekte wird die Cloud als »besseres Rechenzentrum« angesehen und eine tiefgreifende Transformation der Organisation unter Umständen nicht als notwendig erachtet. Die Erreichung der Ziele ist aber in einem solchen Ansatz keineswegs trivial. Die Cloud kann etwa ihre Stärken hinsichtlich Kosteneffizienz und Ausfallsicherheit, die in der dynamischen Skalierung und Provisionierung liegt, nicht ausspielen, wenn die Anwendung ein portierter, statischer Monolith ist, der manuelle Schritte benötigt, um installiert zu werden (Lift and Shift). Außerdem unterliegen viele Geschäftsmodelle einer Versicherung nur bedingt einer ausreichenden Dynamik von Rechnerleistung und Speicherbedarf, die üblicherweise die Skalierungs-Modelle einer Cloud-Nutzung treiben.
- Reduzierung der Time-to-Market und schnellere Service-Einführung für Versicherungskunden: Dieses Ziel – ein weiteres »Paradeversprechen« der Cloud – adressiert insbesondere die durchgängige Agilisierung der Entwicklung eigener Software. Wie erfolgreiche InsurTechs es vormachen, sollen schnell neue Produkte und Services entwickelt, getestet und verworfen oder weiterentwickelt werden können. Als Geschäftsnutzen wird hier das erfolgreiche Teilnehmen an der Economy of Speed und den allgegenwärtigen Ökosystemen gesehen. Zur Erreichung dieses Ziels sind naturgemäß durchgreifende Transformationen und Anpassungen an der Organisation durchzuführen. Die Agilität der Cloud in Entwicklung, Deployment, Betrieb und Skalierung benötigt eine Entsprechung in der Organisation, um voll wirksam zu sein.

Nicht zuletzt ist auch die Kreativität der Organisation, neue Produkte und Services zu erdenken und aus dem Ideenstatus in die Realisierung zu überführen, eine wichtige Voraussetzung für die Zielerreichung. Die Transformation muss mit dem einhergehenden Kulturwandel diese Kreativität fördern oder wenigstens ermöglichen.

Aufgrund der hier skizzierten tiefgreifenden Transformationsanforderungen einerseits und der Attraktivität des dritten Zieles andererseits werden wir im Rest des Kapitels diese Zielvorgabe als Voraussetzung nutzen und die Themen Kultur- und Organisationswandel genauer beleuchten, die für die vollständige Nutzung der Potentiale der Cloud notwendig sind.

2.1 Warum brauchen wir Kultur- und Organisationswandel und was bedeutet das?

Mit der oben angeführten Entscheidung, in die Cloud zu gehen, werden zahlreiche erwartete Vorteile verbunden. Allerdings folgen daraus auch weitere Entscheidungen, die eine Auswirkung auf bisher etablierte Vorgehensweisen, Prozesse und Strukturen in weiten Teilen des Unternehmens inner- und außerhalb der IT haben. Die avisierten Vorteile können nur erzielt werden, wenn gleichzeitig mit einem organisatorischen Wandel auch ein kultureller Wandel in den betroffenen Teilbereichen der Versicherung stattfindet.

Viele der postulierten Vorteile beruhen auf flexibleren Anwendungen und bedürfen eines schnelleren Entwicklungs- und Freigabezyklus, was vor allem durch veränderte Entwicklungsprozesse erreicht werden kann. Das viel gepriesene Modell der Dev(Sec)Ops ist hier eine Grundvoraussetzung für verkürzte Entwicklungszyklen. Stetiges Einholen von Feedback und stetige Zusammenarbeit mit allen Projektbeteiligten und Auftraggebern sind für die Beschleunigung notwendig. Diese Herangehensweise bedarf einer Änderung der gelebten Organisation, um projektorganisierte (»vertikalisierte«), interdisziplinäre Zusammenarbeit zu ermöglichen.

Ein erwarteter Vorteil ist das schnellere Zurverfügungstellen von Infrastrukturkomponenten. Einfach auf die Maske des Cloud-Providers gehen, dort eine neue Instanz generieren lassen und schon hat der Entwickler seine Testumgebung. Es muss hier allerdings eine Abwägung zwischen dem einfachen »zur Verfügung stellen« und den vom Unternehmen vorgegebenen Rahmendaten geben. Werden die Security-Richtlinien eingehalten? Welche Open-Source-Frameworks werden genutzt? Welche Betriebskosten entstehen in der (Test-)Umgebung? Hier gilt es, eine Mischung aus den Gegenpolen zu finden: a) Freiheiten für die Entwickler, um Kreativität und Innovation zu fördern, und b) gegebene Richtlinien des Unternehmens abzubilden. Jedes Extrem führt dazu, dass die erwarteten Vorteile, wenn überhaupt, nur eingeschränkt verwirklicht werden können.

Einhergehend mit der notwendigen organisatorischen Einbettung der Dev(Sec)Ops-Modelle bedarf es auch eines kulturellen Wandels, um mögliche Vorteile zu nutzen. Kreativität wird durch offene Kommunikation gefördert. Direktes Einholen von Feedback, offene Besprechung von Kritik und gemeinsame Arbeit an Verbesserungen mit Hilfe gemeinsamer Ideenfindung. All das erfordert eine angepasste Kultur in den Projektteams. Aus einer offenen, risikobereiten Kultur entsteht Kreativität. Kreativität, auch mal einen ungewöhnlichen Weg zu gehen, eine ungewöhnliche Perspektive einzunehmen und so etwas Innovatives zu erschaffen. Mit diesen innovativen Lösungen ist es dann möglich, das volle Potenzial einer cloudifizierten Umgebung zu erschließen. Welche Parameter ermöglichen diese Kreativität? Wie kann man eine derartige Umgebung erschaffen?

2.2 Wie Organisations- und Kulturwandel Ermöglicher der Transformation werden

Organisatorischer und kultureller Wandel sind Voraussetzungen einer erfolgreichen Transformation hin zu modernen Arbeitsweisen in der Cloud und treiben den Wandel im Idealfall an. Diesen Zusammenhang beschreibt das Gesetz von Conway:

»Organisationen, die Systeme entwerfen, [...] sind gezwungen, Entwürfe zu erstellen, die die Kommunikationsstrukturen dieser Organisationen abbilden.«[1]

Dieser Umstand ist so einfach wie problematisch. Versuchen wir mit unserer existierenden Organisation ein System neu zu entwerfen (oder ein existierendes System umzubauen), in unserem Fall die Cloud-Umgebung und Applikationslandschaft, so wird allein die etablierte Kommunikationsstruktur der Organisation dazu führen, dass wir in Teilen die uns bekannte Welt in der Cloud nachbauen. Wie eingangs beschrieben, haben unterschiedliche Cloud-Strategien verschiedene Ziele. Deshalb ist es wichtig, bereits vor Beginn der Migration zu definieren, welche Ziele mit der Aktivität erreicht werden sollen. Für unterschiedliche Business-Ziele muss auch die Organisationsstruktur auf diese Ziele hin optimiert werden. Das so genannte inverse Conway Manöver kann genau diesem Ansatz dienen. Es erkennt die Notwendigkeit an, die Organisation der Zielsetzung entsprechend aufzustellen, um dann davon zu profitieren, dass sich die technische Lösung, von dieser Struktur getragen, gemäß Conway korrekt entwickeln wird. Erfolgreich wird die Transformation, wenn Organisations- und Kulturwandel parallel stattfinden. Vorgehensmodelle wie Dev(Sec)Ops und agile Softwareentwicklung sind mehr als reine Arbeitsweisen, sie betreffen die grundsätzliche Kultur. Mögliche Fehler werden als Teil der Entwicklung verstanden und der Fokus auf die schnelle und nachhaltige Beseitigung gelegt, statt auf die hundertprozentige Vermeidung.

1 Melvin E. Conway: How Do Committees Invent? In: F. D. Thompson Publications, Inc. (Hrsg.): Datamation. Band 14, Nr. 5, April 1968, S. 28–31 (englisch, melconway.com [abgerufen am 11.03.2022]).

Genauso muss eine »schuldbefreite« Kultur des gegenseitigen Vertrauens Mechanismen implementieren, die Fehler erlaubt und darauf fokussiert ist, diese schnell zu beheben (dies alles innerhalb regulatorischer Anforderungen). Menschen müssen dazu bereit sein, Verantwortung zu übernehmen und Organisationen müssen bereit sein, Fehler zu machen und aus diesen zu lernen.

Gleichzeitiger Kultur- und Organisationswandel verstärkt sich gegenseitig. Doch ist es in der Praxis oft schwierig, gewachsene Strukturen aufzubrechen und Ängste im Team zu nehmen, wo zukünftig neue Aufgaben und Herausforderungen die bekannten Abläufe ändern. Auch bedeuten geänderte Verantwortlichkeiten, dass Parteien Mitspracherecht verlieren. Es ist daher wichtig, rechtzeitig auf diese Problematik einzugehen und mit den betroffenen Parteien ein gemeinsames Zielbild zu erarbeiten. Genauso wie die technische Migration in die Cloud iterativ entwickelt werden muss, ist auch die Organisation immer wieder neu anzupassen, um dem Stand der Migration gerecht zu werden. Gelingt es, das Team so zu involvieren, dass es aktiv an der Gestaltung des neuen Zielbilds mitarbeitet und die Möglichkeit bekommt, seine Vorstellungen einer optimalen Arbeitsweise in die Tat umzusetzen, so stößt man deutlich seltener auf Vorbehalte und Ablehnung gegen die Aktivitäten. Anerkennung und Kritik sollten durch das Team selbst initiiert werden. Peer Recognition ist für die meisten Mitarbeiterinnen und Mitarbeiter motivierender als vom Management verordnetes Lob. Das Management sollte hier nur als letzte Instanz eingreifen. Auch hier gilt: Gute Vorbereitung und ausreichende Ressourcen in Form von Trainings, agilen Coaches und Workshops sind unabdingbar. Eine weitere Methode, um einen Kulturwandel zu begleiten, ist die Verwendung des Dojo Konzepts. Hierbei geht es um die Durchführung eines exemplarischen Projekts mit dem Ziel, die gemachten Erfahrungen im Unternehmen zu verbreiten und so in kleinen Schritten eine Umstellung durch ein (erfolgreiches) Beispiel zu bewirken. Letztendlich ist es wichtig, diesen Kulturwandel im gesamten Unternehmen umzusetzen – auch dort, wo korrekterweise keine agilen Arbeitsweisen und Prozesse etabliert werden müssen. Offenheit und Transparenz beginnen an der Spitze der Hierarchie. Mit Lead-By-Example kann die Unternehmensführung vorleben, wie sie sich die Umstellung der Organisation und der Kultur vorstellt.

Die wichtigste Erkenntnis vor Beginn einer Cloud-Transformation ist, dass Erfolg und Misserfolg in den seltensten Fällen durch technische Details entschieden werden. Dennoch wird oft ein Großteil der Aufmerksamkeit und Ressourcen auf diesen Bereich gerichtet. Stattdessen muss die Transformation ganzheitlich verstanden und ein besonderes Augenmerk auf die Organisation selbst gelegt werden.

2.3 Umgang mit der IT der zwei Geschwindigkeiten

Die ganzheitliche Cloud-Transformation mit notwendigem Wandel von Kultur und Organisation gelingt nicht auf einen Schlag. Gerade Versicherungsunternehmen treten ihre Reise typischerweise ausgehend von einer traditionell geprägten IT-Landschaft an – technologisch, organisatorisch und kulturell.

Doch ist die neue Plattformgrundlage schnell gelegt, der erste Anwendungscluster zügig migriert und das erste Team im agilen Cloud-Modus angekommen. Nun arbeitet ein kleiner Teil der Organisation mit einer Geschwindigkeit und nach Paradigmen, die der traditionellen IT fremd sind. Mit dem Fortschreiten der Transformation wird dieser Anteil sukzessive wachsen, existiert aber nicht losgelöst von der bestehenden IT-Landschaft. Genau wie die schnell und unkompliziert in die Cloud migrierte Frontend-Anwendung weiterhin technische Abhängigkeiten zu Backend-Diensten in klassischen Rechenzentren und Mainframes hat, so müssen für einen erfolgreichen Betrieb Prozesse und Organisation zwischen alter und neuer IT-Welt auch auf nicht-technischer Ebene ineinandergreifen. Die erfolgreiche Cloud-Transformation erfordert deswegen ein geduldiges Vorgehen, das die Übergangsphase der heterogenen IT-Realitäten und ihre Schnittstellen und Integrationen bewusst gestaltet statt nur als notwendiges Übel in Kauf nimmt. Unterschiedliche Bedürfnisse und Rahmenbedingungen müssen dabei auf beiden Seiten adressiert werden: Klassische, risikoaverse Governance mit bewährten Wasserfallprozessen und hierarchischen Strukturen blockieren agile Wertschöpfung in der Cloud. Umgekehrt tragen pauschal verordnete Dev(Sec)Ops-Paradigmen und agile Vorgehensmodelle genauso wenig zu einem stabilen Betrieb der traditionellen, auf Kontinuität und Stabilität ausgerichteten IT-Anteile bei. Zu dieser Moderation gehört auch, dass etablierte Anforderungen und darum herum aufgebaute Kompetenzen aus der klassischen IT beim Schritt in die vermeintliche Cloud-Freiheit nicht unbegründet zurückgelassen werden. Themen wie Datensicherung und Netzwerksicherheit haben auch in der Cloud ihren Platz. Ein Plattform-Team kann hier ein Ansatz sein, Mitarbeiterinnen und Mitarbeiter der klassischen IT mit wertstiftenden Aufgaben für die Cloud zu begeistern und bekannte Qualitätsstandards unter Einsatz neuer Technologien und Paradigmen nicht nur zu wahren, sondern mit Cloud-Mitteln besser zu implementieren.

Dieses Spannungsfeld gilt es unter Einsatz unterschiedlicher Projektmethoden und Einbeziehung aller Beteiligten zu navigieren. Insbesondere muss die gegenseitige Wertschätzung und das Verständnis der integrierten Koexistenz auf beiden Seiten gepflegt werden – interner Konkurrenzkampf strebt der übergeordneten Transformation zuwider. Eine besondere Herausforderung ergibt sich, wenn zur lokalen Beschleunigung der Transformation eine (Teil)Ausgliederung verfolgt wurde. Die losgelöste Organisation erscheint für sich ohne Altlasten beweglich zu sein, eine nachhaltige Integration oder gar Rückführung ins Kernunternehmen setzt aber das Auseinandersetzen mit vermeintlich umschifften Maßnahmen auf beiden Seiten voraus.

Schlussendlich wirken Marktdynamik und Transformationsdruck aber auf Unternehmen und IT als Ganzes – Beweglichkeit nur an der Oberfläche wird für die meisten Geschäftsmodelle nicht reichen. Nur eine insgesamt bewegliche und auf den Kunden ausgerichtete IT hält ein Unternehmen nachhaltig wettbewerbsfähig – die IT der zwei Geschwindigkeiten muss deswegen ein Übergang bleiben. Eine Transformationsinitiative ist schnell gestartet, die Übergangsphase mit ersten Erfolgen bald erreicht. Die eigentliche Herausforderung ist es nun, die Transformation nachhaltig zu Ende zu führen hin zu einer IT, die das kontinuierliche Balancieren zwischen Innovation, Risikofreude sowie Effizienz und Stabilität im Kern verankert hat und übergreifend lebt.

3 Wertschöpfung und Governance – Zusammenarbeit mit bzw. Ausgliederung an SaaS-Anbieter in der Cloud

Um die besten und günstigsten Versicherungsprodukte anzubieten, werden zunehmend Partnerschaften mit InsurTechs und anderen etablierten Dienstleistern eingegangen. Das Management aller Berührungspunkte zum Kunden rückt hier stark in den Fokus. Der Schlüssel hierfür ist der Einsatz von (Big) Data Analytics und modernen Cloud-Technologien, eingebettet in eine Architektur, die echte Omnikanäle in der Zusammenarbeit mit externen Dienstleistern darstellen kann. In Kombination mit der Verschmelzung der »alten« Versicherungsdaten mit langer Historie und der »frischen« Daten aus bereits stark digitalisierten Prozessen erlauben diese Technologien den Shift auf ein neues Level bei SaaS-Angeboten.

In vor-digitalen Zeiten erfolgte die Umsetzung sämtlicher Unternehmensprozesse in-house, sodass eine Versicherung unterschiedliche Fähigkeiten in der Organisation selbst umfänglich »besitzen« musste, um Versicherungsprodukte überhaupt anbieten zu können. Dieses Bild einer klassischen Versicherung ändert sich zunehmend hin zu einer Versicherung, welche viele ihrer Teilprozesse an andere Unternehmen »outsourced« und über clevere SaaS-Lösungen und / oder mit adäquaten Schnittstellen in Prozesse einbettet. Ein Beispiel hierfür sind Telematik-Autoversicherungspolicen, die sich im Markt etabliert haben. Sie zeigen, dass smarte Produkte, die Umweltaspekte und Technologie verbinden, neue Werte kreieren. Software ist hier klar ein Hebel, den Wert von Daten zu monetarisieren. In diesem Zusammenhang wirkt die Cloud-Technologie wie ein Treibsatz. Sie ermöglicht sowohl die Skalierung als auch die Verkürzung der Time-to-Market – die Einführung neuer Dienstleistungen und Produkte in Wochen und nicht Monaten.

Für die Einführung eines solchen grundlegend flexibleren Geschäftsmodells mit unterschiedlichen SaaS-Lösungen ist eine smarte Governance unerlässlich. Sie muss den dafür nötigen Rahmen schaffen, um gleichzeitig hoch-regulierten Unternehmen, wie Versicherungen, die nötige (Rechts-) Sicherheit und Compliance bieten zu können. Die Governance muss aber auch dieses schlanke, agile und vor allem datengetriebene Produktionsmodell möglich machen: das rasche Implementieren von Produkten und Services, das Testen, aber auch das Ändern und Abmanagen – kurz; die Optimierung der Wertschöpfung absichern.

3.1 Der Blick auf die Wertschöpfungskette

Durch die angesprochene Vereinfachung, Prozessschritte oder ganze Teilprozesse an digital orientierte Business Process Outsourcer (BPOs) oder SaaS-Anbieter auslagern zu können, haben Versicherungen nun vielmehr die Möglichkeit, sich auf ihre Kernkompetenzen und die Orchestrierung der Wertschöpfungskette zu fokussieren. Diese Orchestrierung wird damit natürlich erheblich komplexer und eine solche Governance muss vorab gut durchdacht und als entsprechender Aufwand berücksichtigt werden. Wenn man dafür beispielhaft die Wertschöpfungskette von KFZ-Versicherungen betrachtet, wird auch schnell klar, was damit gemeint ist:

Die tatsächliche Wertschöpfung von Versicherern beschränkt sich auf eine Hand voll essenzieller Teilaspekte. Den »Rest« können sie auslagern und damit abgeben, aber auch verbessern, wie das Beispiel Risikobewertung zeigt. Über entsprechende Anbieter betten Versicherer eine Vielzahl an spezifischen Daten mit darunterliegenden automatisierten Auswertungen einfach in den eigenen Prozess ein. Damit können sie flexibel und schnell eine Wertschöpfung darstellen, die sie in »Eigenbau« nur unter großem Aufwand und in jahrelanger Entwicklungsarbeit erreicht hätten. Das entlastet auch Sachbearbeiter und Vermittler, die nunmehr wieder vermehrt den Kunden durch persönliche Betreuung in den Vordergrund stellen können.

Ein weiteres Beispiel und zentraler Ansatzpunkt für die Digitalisierung einer Versicherung ist es, ein altes Schadensystem – nicht selten eine Mainframeanwendung – durch ein Cloud-basiertes System abzulösen. So wird zwar ein Teil der Gesamtwertschöpfung in der Kette an einen SaaS-Anbieter abgegeben, gleichzeitig öffnen sich jedoch neue Türen. Die reibungslosere Koordination von Aufträgen an Dienstleister, wie zum Beispiel Werkstatt-Vermittler oder Gutachter, die heute meist umständlich über teils ungesicherte Wege elektronisch übertragen werden, ist so mit neuesten technischen und fachlichen Standards möglich, auch unter Berücksichtigung von Security-Aspekten. Auch die Rückübertragung von Informationen gelingt so ohne Hürden. Die Aufgabe des Versicherers liegt also künftig vor allem darin, eine Governance für diese dekonstruierte Wertschöpfung zu entwickeln und umzusetzen, die einen Rahmen bietet für:

- schlanke Prozesse mit Potential zur Auslagerung sowie die Entwicklung externer Unterstützung
- strategisch richtige SaaS-Partner und »digitale« BPOs finden und einbinden
- Kernkompetenzen identifizieren und »schützen«, um die Daseinsberechtigung zu bewahren
- Process-Owner und Zugehörigkeiten (Daten, Anwendungen, etc) definieren
- Compliance Anforderungen (Regulatorik) über alle externen Partner hinweg zu sichern

Die neue Governance schafft somit einen Ordnungsrahmen in einer mehr und mehr zerstückelten Wertschöpfungskette. Mit dieser Fragmentierung ergeben sich für eine Versicherung sowohl Risiken als auch Chancen, wobei beides zumindest in der Übergangszeit mit spezialisierten IT-Dienstleistern als Beratungs- und Implementierungspartnern an der Seite optimiert werden kann. Diesen Spezialisten in der Branche kommt in den nächsten Jahren besondere Bedeutung zu: Sie müssen die Entwicklung von Software, beispielsweise von Schnittstellen zu den Cloud-Anbietern, trotz De-Globalisierung sicherstellen. Sie müssen die neuen Formen der Produktion innerhalb der Versicherungen mit ihren eigenen Produktionsmodellen per default synchronisieren können, um die gewollten Innovationen über Standard-Plattformen in time zu liefern, auch in den Ausschnittslösungen, welche die jeweiligen Strategien der einzelnen Versicherungen fordern. Agile Standards in Kombination mit Dev(Sec)Ops sind für diese Dienstleister und SaaS-Anbieter somit unerlässlich.

3.2 Chancen und Risiken

Gute Governance beinhaltet die genannten Kernkompetenzen und deren Schutz. Nur so bewahren Versicherer die Hoheit über die fachlichen Prozesse und verhindern, dass die Versicherung selbst zum reinen Produktlieferanten in einem (aus Kundensicht) zunehmend heterogen Markenumfeld degradiert wird, indem große Teile der eigenen Wertschöpfungskette ausgelagert werden. Auch die Abhängigkeit von einzelnen SaaS-Anbietern sollte ein gesundes Maß nicht überschreiten (Exit Strategie, Zwei-Anbieter-Strategie, ...). Große Versicherungen setzen in der Regel auf große, etablierte SaaS-Anbieter. Im Hinblick auf die Stabilität der Services und der dahinterstehenden Unternehmen kann das Sinn ergeben, dafür ist man abhängiger von den Produktstrategien der Anbieter. Kleine InsurTechs hingegen locken mit innovativen, maßgeschneiderten Produkten, bergen jedoch das Risiko von Instabilität. Grundsätzlich sind hier Merger & Acquisitions eine Option, sich Innovationen zu sichern. Die gesparten Entwicklungs- und RampUp-Kosten in Relation zu dem erwartbaren Nutzen in Effizienz und Wettbewerbsfähigkeit – eine solche Strategie kann sehr erfolgversprechend sein. Es zeigt sich: Dort, wo Risiken sichtbar werden, sind auch Chancen zu finden, die nicht nur das Geschäftsmodell der Versicherung, sondern auch das Produktangebot für den Endkunden erheblich verbessern können. Neben der Kosteneinsparung durch die Auslagerung von Teilprozessen, können die freiwerdenden Ressourcen, in der Regel Mitarbeiter mit Versicherungsspezifischem Knowhow, an der Erweiterung und Verbesserung der Wertschöpfungskette arbeiten.

3.3 Die zukünftige Rolle einer Versicherung

Versicherer, die ihre SaaS- und BPO-Partner geschickt nutzen und einbinden, verändern ihre Kundenbeziehung grundlegend. Beispielsweise sind sie im Schadenfall für den Kunden immens wichtig: Auf das Management der Regulierung, das Management dieser Beziehungssituation besonderen Wert zu legen, zahlt sich in Schadenfällen aus. Darüber hinaus können Versicherungen durch die Einbindung von solchen Lösungen ihr eigenes Angebot und auch die Kontaktpunkte zu Kundinnen und Kunden weiter vergrößern. Mehrwertdienste, personalisierte Angebote und Ratschläge rund um das versicherte Produkt sind nur einige Beispiele. Die Zusammenarbeit mit ausgewählten Partnern kann hier zu einer erfolgreichen Dreiecksbeziehung führen, in der der Endkunde von neuartigen Services profitiert, und die Versicherung ihre Kundenbindung und den Share-of-Wallet stärkt.

Konkret sind in dieser Beziehung die ersten Schritte bereits gegangen: Telematik-KFZ-Tarife sparen nicht nur der Versicherung, sondern auch den Kundinnen und Kunden Kosten. Die transparente Darstellung des eigenen Fahrverhaltens kann dieses darüber hinaus positiv beeinflussen und so die Straßensicherheit erhöhen. Die Auswertungen anonymisierter Fahrdaten ermöglichen zudem weitere Angebote und Kooperationen. Sei es mit Werkstätten, Autobauern oder bei Unfällen mit Behörden. Analog zum Telematik-KFZ-Tarif ermöglichen auch Wearables und Smart Home Produkte vielseitige Möglichkeiten, alte Versicherungsprodukte neu zu denken bzw. die Wertschöpfungskette der klassischen Versicherung zu erweitern. Gute Governance, sei es in Bezug auf Kundendaten oder aber auch auf die Hoheit über fachliche Prozesse, schützt hier nicht nur den Endkunden, sondern auch die Versicherung.

3.4 Zusammenfassung

Der Weg zum nachhaltigen Erfolg führt Versicherer also zu einer Vielzahl an potentiellen SaaS- und digitalen BPO-Partnern. Die große Aufgabe, die auch maßgeblich zwischen Bestehen und Scheitern entscheidet, ist es, eine Governance zu entwickeln, die langfristig einen optimalen Rahmen zur Anbindung von externen Anbietern und der Fortentwicklung der eigenen Kernkompetenzen sicherstellt. Das Ziel der Transformation des eigenen Geschäftsmodells muss sein:

- den Wettbewerbsvorteil gegenüber der Konkurrenz beizubehalten und möglichst zu vergrößern,
- die internen Prozesse kontinuierlich zu optimieren,
- »unliebsame Themen« auslagern und so Risiken zu minimieren.

Es geht abstrakt gesprochen um eine Neuausrichtung des Geschäftsmodells auf Basis der Analyse und Bewirtschaftung von großen Datenmengen. Neue SaaS-Anbieter und die Anbindung durch Cloud-Technologie sind hier der Hebel für gesicherte Erlöse bei weniger Risiko. Es geht um mehr try-and-error und nicht um bloßes Exekutieren bei der Etablierung von datengetriebenen Produktionsmodellen. Das bedingt eine smarte Governance und neue Modelle in der Zusammenarbeit mit IT-Dienstleistern. Eine so gedachte und gebaute Wertschöpfungskette fokussiert sich auf den Nutzen für den Kunden: sowohl bei den Kosten als auch neuen, smarten Produkten und Services. Das ist auf lange Sicht ausgesprochen positiv und ein starker Treiber im Markt.

4 Fazit

Wie bei allen strategischen IT-Fragestellungen lässt sich das Thema Cloud nur im Zusammenhang mit der technologischen Gesamt-Transformation und natürlich dem Geschäftsmodell der jeweiligen Versicherung ausdetaillieren. Klar ist aber auch, dass zumindest die Herstellung einer „Cloud-fähigen« Organisation inzwischen fester Bestandteil jeder IT-Strategie ist oder sein sollte: Moderne Architekturen und Frameworks für die Software-Entwicklung, ein zeitgemäßer IT-Betrieb („DevSecOps«), Zugriff auf und flexible Interaktion mit technologisch ausgerichteten Dienstleistern und Partnern, beabsichtigte Nutzung von AI etc. – all diese Themen sind eng mit dem Thema Cloud-Infrastruktur verknüpft, teilweise daraus entstanden.

Diese eher technischen Begriffe spiegeln sich in Themen, die gängigen geschäftlichen Strategiebestandteilen entsprechen: Agilität in der Organisation, Teilnahme an bzw. der Aufbau eigener Ökosysteme, BPO an technologisch versierte Partner, Omnikanal-Vertrieb und -Kundenbetreuung etc.: IT und Cloud »stecken nicht dahinter«, sondern sind eng mit all diesen Themen verwoben, in vielen Fällen liefern sie den maßgeblichen Teil der neuen Wertschöpfung. Ein weiterer Hinweis dafür, dass die immer noch unterschwellige IT-Rolle (Fachbereiche schöpfen Wert, IT liefert nachgelagert »zu«) dringend einer Überarbeitung bedarf. Am besten, man streift diese alte IT-Sicht ab.

Womit schlussendlich die Unternehmenskultur auch über der Cloud-Thematik steht: Als fester Bestandteil jeder IT-Strategie unterliegt sie ähnlichen kulturellen Transformationsbedarfen und Stolperfallen. Die gute Nachricht: Die nachhaltige Planung und transparent kommunizierte Umsetzung einer »Cloud-fähigen« Organisation eignet sich gut als Blaupause für einen großen Teil der Gesamt-Transformation einer IT, inklusive vieler Themen im Rahmen der Einführung von Agilität im Unternehmen. Ob eigener Betrieb einer Cloud-fähigen Architektur, Nutzung einer Managed Private Cloud oder eines Hyperscalers; dies ist dann tatsächlich eine nachgelagerte Frage.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom