de:hub
digital ecosystems

InsurLab Germany

CLOUD PUSH:
Für eine erfolgreiche Zusammenarbeit zwischen Versicherungen und Start-ups

Whitepaper des Insurlab Germany
in Zusammenarbeit mit unseren
Mitgliedern und Partnern

INHALTSVERZEICHNIS

AUTOREN & AUTORINNEN

Klemens Hägele, IBM
Martin Harasim, AWS
Sebastian Brück, InsurLab Germany
Oliver Schaber, ROLAND Rechtsschutz-Versicherungs-AG
Tim Oberthür, ROLAND Rechtsschutz-Versicherungs-AG
Peter Pillath, Parametrix Insurance
Ralf Hörnig, Gothaer
Matthias Grasser, Alte-Leipziger Hallesche
Claes Horsmann, IBM
Foelke Hellmich, HDI Global Specialty SE & HDI Global SE

VORWORT

Liebe Leserinnen und Leser,

bereits kurz nach der Gründung des InsurLab Germany e.V. haben wir im Jahr 2019 unsere erste Topic Group zum Themenbereich der Nutzung von Cloud-Technologie durch Versicherungen ins Leben gerufen. Unser erklärtes Ziel war und ist es, Versicherungsunternehmen bei der Nutzung und Implementierung von Cloud-Technologien durch offenen und zugleich vertraulichen Austausch zu unterstützen.

In unseren Topic Groups versammeln sich ausgewiesene Expertinnen und Experten aus zahlreichen Mitgliedsunternehmen der Versicherungswirtschaft, unseren beiden Technologiepartnern AWS und IBM sowie innovativen Start-ups, um Themen von gemeinschaftlichem Interesse zu erarbeiten.
In den ersten beiden Jahren konzentrierten wir uns in der Topic Group Cloud vornehmlich auf die Herausforderungen der Regulatorik, Technologie, Resilienz und Sicherheit, insbesondere der VAIT (Versicherungsaufsichtlichen Anforderungen an die IT) und den damals frisch veröffentlichten Leitfaden des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) in Bezug auf die Cloud-Nutzung.

Nach drei Jahren (trotz Corona) regelmäßiger (Online-) Treffen und intensiven Austauschs in der Topic Group Cloud-Push möchten wir als Gruppe die im Kollektiv vorhandene Expertise auch für einen breiteren Kreis zugänglich machen, da wir die Interaktion als sehr wertvoll und hilfreich erlebt haben. Die erfolgreiche Nutzung von Cloud-Technologie wird mehr und mehr zum kritischen Business-Enabler. Zahlreiche Lösungsansätze von Start- und Scale-ups basieren auf Cloud-Infrastrukturen, wobei dieses eher technische Thema sowohl erste Herausforderung als auch Einstieg in eine fruchtbare Zusammenarbeit im Versicherungsumfeld sein kann.

Das vorliegende Dokument zielt darauf ab, die Kooperation zwischen Start- und Scale-ups einerseits sowie Versicherungen andererseits in Bezug auf Cloud-Nutzung zu erleichtern. Wir ermutigen euch, IT-Prozesse neu zu denken, die Möglichkeiten von Cloud-Anwendungen zu eruieren und wollen ein tiefergehendes Verständnis für unterschiedliche Perspektiven vermitteln. Mit der richtigen Herangehensweise und guten Partnern überwiegen die Chancen und Nutzen die Herausforderungen.
Für Rückfragen oder Anmerkungen stehen wir und die jeweiligen Autorinnen und Autoren dieses Werkes euch gerne zur Verfügung. Viel Spaß bei der Lektüre!

Herzliche Grüße

Martin Harasim,
Klemens Hägele &
Sebastian Brück

MARTIN HARASIM

KLEMENS HÄGELE

SEBASTIAN BRÜCK

1 EINLEITUNG

Motivation - Grundgedanken des Whitepapers

Dieses Whitepaper ist ein Einstieg in das Thema der Nutzung von Public Cloud und SaaS-Angeboten und richtet sich vor allem an Start-ups und Versicherungsunternehmen, um einen Überblick über die wichtigsten Inhalte für den erfolgreichen Einsatz von Cloud-Technologie zu geben. Es ist ein Leitfaden für die Schwerpunktthemen Cloud, Security und Compliance.

Es handelt sich nicht um eine abschließende und vollumfassende Bewertung des Cloud-/SaaS-Marktes. Für jedes Unternehmen müssen Aufwand und Nutzen individuell betrachtet werden. Gleichzeitig hilft dieses Whitepaper dabei, sich grundsätzliche Fragen zu stellen und auch Bedürfnisse des Gegenübers (Versicherungsunternehmen/Start-up) zu betrachten.

Es werden dazu gezielt Fragen und Aufgabenstellungen aufgezeigt und Ideen an die Hand gegeben, anstatt feste Antworten für alle Punkte zu formulieren, da jedes Unternehmen unterschiedliche Lösungsansätze benötigt. Die abzudeckenden Themen sind jedoch identisch.

In diesem Whitepaper konzentrieren wir uns auf Angebote innerhalb der Public Cloud. Aufgrund des Funktionsumfangs und der Handhabbarkeit ist die Public Cloud die Basis der meisten Angebote und Grundlage von SaaS-Diensten. Der Markt wird dominiert von den großen amerikanischen Anbietern. Um den rechtlichen Bestimmungen, insbesondere dem Datenschutz, gerecht zu werden, betreiben alle großen Anbieter Rechenzentren in Europa. Gleichzeitig erhöht sich das Angebot an europäischen Anbietern, welche in den Markt drängen.

Auf der Suche nach den richtigen Partnern

Große Unternehmen haben langwierige Abstimmungsprozesse und viele Bereiche, die bei strategischen Entscheidungen berücksichtigt werden müssen. Oftmals ist es hilfreich, bei der Einführung von neuen Technologien einen Blick von außen einzubeziehen, der nicht eingeschränkt durch interne Erfahrungswerte ist. Nur so können bestimmte Bereiche vollständig neu gedacht werden.

Die Herausforderung ist dann, die "alte" und "neue" Welt zu einer funktionierenden zusammenzubringen. Umso wichtiger ist die Wahl der richtigen Partner. Ein Start-up als Partner kann als Schnellboot agieren, welches in kleinen Bereichen auch mal etwas ausprobieren und falls nötig zügig die Richtung wechseln kann. Interagiert ein Start-up mit mehreren Partnern, profitiert das einzelne Versicherungsunternehmen von den bereits gemachten Erfahrungen.

Die Reise in die Cloud

Versicherungsunternehmen haben ein seit Jahrhunderten bestehendes und funktionierendes Geschäftsmodell. Dieses muss nicht neu erfunden werden, die Wertschöpfung und die Prozesse müssen sich jedoch den neuen Marktentwicklungen sowohl auf Technologieseite als auch auf Kundenseite anpassen.
Die digitale Transformation und damit einhergehend eine passende Cloud-Strategie ist eine Managementaufgabe für die höchste Führungsebene im Unternehmen. Die Digitalisierung nimmt inzwischen einen solchen Stellenwert ein, dass es sich ein Unternehmen nicht erlauben kann, die IT-Infrastruktur entkoppelt von der damit verbundenen langfristigen Unternehmensausrichtung separiert von anderen Geschäftsentscheidungen zu betrachten.

Eine erfolgreiche Cloud-Einführung beinhaltet den Eingriff in bestehende und teils kritische Prozesse, und betrifft insbesondere auch die Arbeitsweisen der Mitarbeiter und Mitarbeiterinnen. Daher ist die detaillierte Planung und die Begleitung durch ein Change-Management, insbesondere für die Themen Security und Compliance, sowie die Kosten- und Kapazitätsplanung entscheidend.
Eine Stärke der Traditionsunternehmen liegt in der bereits erfolgten Umsetzung von Governance-Anforderungen in funktionierende, sichere IT-Lösungen, die compliant sind und einem Audit standhalten. Hier können und müssen die Versicherer Rahmenbedingungen schaffen, in die Start-ups "reinarbeiten" können.

Kommt es aufgrund von Sonderereignissen, wie etwa einem Cyber-Angriff oder Brand in dem hauseigenen Rechenzentrum, zu kurzfristigen Entscheidungen den Weg in die Cloud zu gehen, ist der Entscheidungsspielraum für geeignete Partner stark eingeschränkt und der Planungshorizont minimiert.

In diesem kompakten Leitfaden werden (ohne Anspruch auf Vollständigkeit) die wesentlichen Fragestellungen gesammelt, die es in der Zusammenarbeit von InsurTechs und Versicherungsunternehmen zu berücksichtigen gilt.

2 REGULATORIK

GRUNDLAGEN ZUR REGULATORIK IM KONTEXT DES CLOUD COMPUTINGS

Der Begriff ‚Regulatorik' umfasst alle gesetzlichen und aufsichtsrechtlichen Anforderungen, die von Unternehmen erfüllt werden müssen. Auch Im Bereich der Versicherungswirtschaft gibt es eine Vielzahl von regulatorischen Anforderungen. Diese gelten dabei nicht nur für die Verwendung von Cloud-Services, die z. B. von Hyperscalern wie AWS, IBM etc. erbracht werden, sondern auch für jede Art von IT-Diensten, die für einen Versicherer extern erbracht werden. Die Nutzung von Cloud Computing Services stellt für Versicherungsunternehmen und ihre Wertschöpfungspartner eine Herausforderung dar, da die Daten und Prozesse nicht mehr bei vollständiger Kontrolle auf eigenen Servern, sondern auf den Servern von Cloud-Anbietern gespeichert und verarbeitet werden, woraus spezifische Risiken mit Informations- und IT-Sicherheitsrelevanz resultieren. Die geltenden regulatorischen Anforderungen dienen dazu, diese Risiken zu minimieren und die Daten und Informationen der Versicherungsunternehmen und ihrer Kundinnen und Kunden zu schützen.

Hauptziele mit Blick auf die IT-Sicherheit sind die Gewährleistung der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität geschäftsrelevanter Informationen. Auch der Datenschutz zählt mit dem übergeordneten Ziel des Schutzes personenbezogener Daten zu Daten und Prozessen von Versicherungsunternehmen und ihren Kundinnen und Kunden. Um diese Ziele zu erreichen, müssen die Versicherungsunternehmen sowie ihre Partnerunternehmen und Dienstleister eine Vielzahl von technischen und organisatorischen Maßnahmen umsetzen.

Auch Start-ups können dabei die Rolle solcher Partnerunternehmen und Dienstleister einnehmen. Aus diesem Grund ist die Differenzierung der Perspektiven auf die Regulatorik aus der Sicht des Versicherungsunternehmen sowie des Start-ups von zentraler Bedeutung. Dafür sind nachfolgend einige Gedankenimpulse aufgeführt.

ZUSAMMENARBEIT VON START-UPS UND VERSICHERUNGSUNTERNEHMEN

Der Einsatz von Cloud-Services bietet Unternehmen, einschließlich Versicherungsunternehmen, viele wirtschaftliche Vorteile wie Skalierbarkeit, Flexibilität und Kosteneinsparungen. Gleichzeitig müssen Chancen und Risiken im Hinblick auf Datenschutz und Informationssicherheit bewertet werden. Durch die Nutzung von Cloud-Services werden die Daten des Versicherungsunternehmens, seiner Partnerunternehmen und seiner Kundinnen und Kunden außerhalb der eigenen IT-Infrastruktur gespeichert und verarbeitet. Dies führt zu einer Neubestimmung der Unternehmensposition bzgl. Cyberangriffen, Datenschutzverletzungen und Datenverlusten. Darüber hinaus können regulatorische Anforderungen aufgrund der Nutzung von Cloud-Services erheblich komplexer und schwieriger zu erfüllen sein. Dabei sind vor allem bei internationalen Cloud Computing- und Outsourcing-Aktivitäten die spezifischen regulatorischen Anforderungen des im Ausland sitzenden Leistungspartners zu berücksichtigen.

Somit besteht ein Trade-off zwischen dem wirtschaftlichen Nutzen und den damit verbundenen Risiken. Es ist wichtig, dass Unternehmen geeignete Maßnahmen ergreifen, um das Risiko von Datenschutzverletzungen und Cyberangriffen zu minimieren und eine angemessene Sicherheits- und Compliance-Kultur aufzubauen. Dazu gehört auch die sorgfältige Auswahl von Cloud-Service-Providern und die Festlegung klarer Verantwortlichkeiten und Vertragsbedingungen in Bezug auf Datenschutz und Informationssicherheit.
Start-ups können als Anbieter von "Managed Software-as-a-Service"-Angeboten auftreten. Das Versicherungsunternehmen konsumiert in diesem Fall die angebotenen Services unmittelbar und ist selbst nicht für den Betrieb der zugrundeliegenden Infrastrukturen verantwortlich. Diese werden entweder durch das Start-up betrieben oder von diesem als von Drittanbietern betriebene "Infrastructure-as-a-Service"-Dienste genutzt.

Weiterhin können die Start-ups als Hersteller der durch die Versicherungsunternehmen selbst zu betreibenden Anwendungen und Services auftreten. Dabei wird meist Software durch das Start-up zur Verfügung gestellt und das Leistungsspektrum kann um Updates und Wartungen erweitert werden. Der Betrieb beim Versicherer erfolgt auf der Grundlage einer durch diesen betriebenen Infrastruktur.

Eine dritte Perspektive ist die der Beratung, bei der Start-ups einer Versicherung eine Beratungsleistung unter der Verwendung von Cloud-Services erbringen. Hierbei kann das Start-up selbst "Software-as-a-Service"-Dienste von Drittanbietern nutzen, oder es kann eine Mischform der zwei zuvor beschriebenen Anwendungsfälle zum Einsatz kommen.

Grundsätzlich sind sowohl das Start-up als auch das Versicherungsunternehmen dafür verantwortlich, sicherzustellen, dass die regulatorischen und gesetzlichen Anforderungen eingehalten werden. Das Versicherungsunternehmen ist in der Regel der "Datenverantwortliche" im Sinne der Datenschutz-Grundverordnung (DSGVO) und trägt damit die (Haupt-) Verantwortung für die Einhaltung von Datenschutz- und Informationssicherheitsanforderungen.

Das Start-up hingegen ist als Dienstleister verpflichtet, die bereitgestellten Cloud-Services so zu gestalten und zu betreiben, dass die Anforderungen der Versicherungsunternehmen erfüllt werden. Das bedeutet, dass das Start-up sicherstellen muss, dass seine Dienste den geltenden rechtlichen und regulatorischen Anforderungen entsprechen und geeignete technische und organisatorische Maßnahmen zur Informationssicherheit und Datenschutz umsetzt. Der Versicherer als Verantwortlicher ist verpflichtet, die regelkonforme Umsetzung durch das Start-up zu prüfen.

Es ist wichtig, dass die Zusammenarbeit zwischen Start-up und Versicherungsunternehmen von Beginn an von einem engen Austausch geprägt ist, um sicherzustellen, dass beide Parteien ihre Pflichten erfüllen und ein hohes Maß an Compliance gewährleistet ist. In der Praxis ist es jedoch oft so, dass das Versicherungsunternehmen eine stärkere Verantwortung trägt, da es in der Regel der primäre Ansprechpartner für Regulierungsbehörden und Aufsichtsorgane ist.

WICHTIGE REGULATORISCHE ANFORDERUNGS-KATALOGE FÜR START-UPS UND VERSICHERUNGS-UNTERNEHMEN IM CLOUD-KONTEXT

Im Bereich der Versicherungswirtschaft gibt es eine Vielzahl von gesetzlichen Vorgaben und Verpflichtungen, die von den Versicherungsunternehmen und ihren Partnern eingehalten werden müssen. Dazu gehören unter anderem die nachfolgend aufgeführten zentralen Beispiele für gesetzliche und regulatorische Anforderungen.

Orientierungshilfe zur Auslagerung an Cloud-Anbieter
(Stand November 2018)

Die Orientierungshilfe zur Auslagerung an Cloud-Anbieter der BaFin gibt konkrete Hinweise, wie Versicherungsunternehmen bei der Zusammenarbeit mit Cloud-Providern vorgehen sollten. Sie soll den Unternehmen helfen, die regulatorischen Anforderungen zu erfüllen und die besonderen Risiken bei der Auslagerung an Cloud-Provider zu minimieren. Veröffentlicht wurde die Orientierungshilfe im Juni 2017 und sie ist somit auch ein recht aktuelles Anforderungspapier.

Mindestanforderungen an die Geschäftsorganisation MaGo
(Januar 2018 - Rundschreiben BaFin zur MaGo 08/2020)

Die Mindestanforderungen an die Geschäftsorganisation (MaGo) der BaFin stellen eine weitere wichtige regulatorische Anforderung dar. Sie legen fest, dass Unternehmen, die IT-Dienstleistungen auslagern, ein effektives Risikomanagement-System implementieren müssen, um Risiken bei der Auslagerung zu minimieren. Hierbei sind insbesondere die Auswahl geeigneter Cloud-Provider, die Absicherung von Daten sowie die Wahrung der Vertraulichkeit und Integrität von Daten von großer Bedeutung. Die MaGo wurde am 1. Januar 2018 veröffentlicht.

Bundesdatenschutzgesetz BDSG (neu)
(alte Fassung Januar 1978, neue Fassung Mai 2018)

Das Bundesdatenschutzgesetz (BDSG (neu)) ist das nationale Datenschutzgesetz in Deutschland und regelt den Umgang mit personenbezogenen Daten. Es stellt sicher, dass Unternehmen personenbezogene Daten nur unter klar definierten Vorgaben speichern und verarbeiten dürfen. Es enthält detaillierte Vorschriften zur Datensicherheit und zum Datenschutz, einschließlich der Verpflichtung zur Ernennung eines Datenschutzbeauftragten und zur Durchführung regelmäßiger Datenschutzfolgenabschätzungen.

EU-DSGVO
(Mai 2018)

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) ist eine umfassende Verordnung zum Schutz personenbezogener Daten, die in allen EU-Mitgliedstaaten gilt. Sie stellt sicher, dass personenbezogene Daten nur in Übereinstimmung mit dem Grundsatz der Datensparsamkeit und dem Recht auf Informationssicherheit verarbeitet werden. Unternehmen müssen eine klare Einwilligung der betroffenen Personen einholen, bevor sie personenbezogene Daten speichern oder verarbeiten. Die Verordnung verlangt auch, dass Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten zu schützen.

EIOPA Leitlinie IKT
(Februar 2018 Leitlinien einschließlich 08/2022)

Die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) hat Leitlinien zu Informationstechnologie und Kommunikation (IKT) veröffentlicht. Die Leitlinien stellen sicher, dass die Versicherungsunternehmen über ein angemessenes Management von IKT-Risiken verfügen, um die Stabilität und Kontinuität der Geschäftstätigkeit sicherzustellen. Sie enthalten Vorgaben zur Implementierung von Maßnahmen zur Gewährleistung von Datensicherheit und Datenschutz sowie Empfehlungen zur Risikobewertung und zum Management von Cyber-Risiken.

ESMA Auslagerungen an Cloud-Anbieter
(Stand: 05/2021)

Die European Securities and Markets Authority (ESMA) hat Leitlinien zur Auslagerung von Aktivitäten an Cloud-Computing-Anbieter veröffentlicht. Die Leitlinien legen Anforderungen an die Auslagerung von Aktivitäten an Dritte fest und betreffen insbesondere die Einhaltung von Datenschutz- und Datensicherheitsvorschriften sowie die Notwendigkeit, interne Kontrollen und Risikomanagementverfahren aufrechtzuerhalten. Sie enthalten auch Empfehlungen für die Gestaltung von Verträgen mit Cloud-Computing-Anbietern, die angemessene Schutzmaßnahmen und Rückgriffsrechte für das auslagernde Unternehmen gewährleisten sollen.

Versicherungsaufsichtliche Anforderungen an die IT
(Erste Fassung Oktober 2018, aktuelle Fassung März 2022)

Zuletzt sind auch die versicherungsaufsichtlichen Anforderungen an die IT (VAIT) der BaFin von großer Bedeutung. Sie umfassen die gesamte IT-Infrastruktur eines Versicherungsunternehmens und stellen sicher, dass ein effektives IT-Risikomanagement implementiert wird. Die Anforderungen sind seit dem 1. Oktober 2018 in Kraft und wurden zuletzt im März 2022 aktualisiert. Bei der Zusammenarbeit mit Cloud-Providern müssen die Versicherungsunternehmen sicherstellen, dass auch hier die Anforderungen der versicherungsaufsichtlichen Anforderungen an die IT erfüllt werden.

EU Data Act 2022/2023

Der Entwurf eines EU Data Act ((DA)KOM (2022) 68 final) ist Teil der umfassenderen Datenstrategie der Europäischen Union und befasst sich mit diesem Thema, indem er Vorschriften vorschlägt, die den Zugang zu und die Nutzung von Daten, die von Internet-of-Things-Geräten und damit verbundenen Diensten erzeugt werden, durch Unternehmen, Behörden und Einzelpersonen erleichtern. Ziel ist die Schaffung eines europäischen Binnenmarktes für Daten (COM (2015) 192 final). Das Datengesetz schlägt auch wichtige Änderungen vor, um den Wechsel von Cloud-Diensten zu erleichtern. Das Datengesetz soll es den Kunden von Cloud- und Edge-Diensten auch erleichtern, zwischen Cloud-Anbietern zu wechseln, die dieselbe Art von Dienst anbieten. Dies geschieht, indem Cloud-Anbieter verpflichtet werden, kommerzielle, technische, vertragliche und organisatorische Hindernisse zu beseitigen.

Digital Operational Resilience Act (Jan 2023)

2020 hat die Europäische Kommission den ersten Entwurf des "Digital Operational Resilience Acts" (DORA) veröffentlicht (seit 16.01.2023 in Kraft; muss noch in nationales Recht umgesetzt werden). Durch die Neuerungen wird ein stärkerer Fokus auf die Informations- und Kommunikationstechnik (IKT) -Strategie und deren Widerstandsfähigkeit gelegt. Die zusätzlichen Anforderungen sehen vor, dass eine Sensibilität für IKT-Risiken und deren Auswirkungen im gesamten Unternehmen geschaffen wird und Drittanbieter in die IKT-Risikobewertung integriert werden Neue Berechtigungen seitens der Finanzdienstleister und Aufsichtsbehörden: Einführung von Strafzahlungen und neue Kündigungsoptionen wegen Nichteinhaltung sowie umfassende Prüf- und Zugriffsrechte auf Dienstleister und Cloud-Anbieter

Der Artificial Intelligence Act (AIA) liegt im Entwurf seit dem 21. April 2021 vor
(Inkrafttreten voraussichtlich 2024)

Er zeichnet sich durch seine weitreichende Definition von KI-Systemen und die Auferlegung umfangreicher Dokumentations-, Schulungs- und Überwachungsanforderungen für KI-Tools aus, die in seinen Geltungsbereich fallen. Jedes Unternehmen, das auf dem EU-Markt tätig ist und Software auf der Grundlage von maschinellem Lernen entwickelt oder einführen möchte, wird von dem AIA betroffen sein. KI hilft bei der Automatisierung von Routinetätigkeiten innerhalb der IT-Infrastruktur; dies erhöht die Produktivität. Die Kombination von KI und Cloud Computing führt zu einem umfassenden Netzwerk, das in der Lage ist, riesige Datenmengen zu speichern und dabei kontinuierlich zu lernen und sich zu verbessern.

ZENTRALE FRAGESTELLUNGEN ZUR ERREICHUNG REGULATORISCHER KONFORMITÄT

Um die Erfüllung regulatorischer Anforderungen im Kontext des Cloud-Computings zu erleichtern, können sich Verantwortliche innerhalb der jeweiligen Unternehmen bestimmte Fragen stellen.

Für ein Start-up können zum Beispiel folgende Fragen relevant sein:

- Wie können Start-ups grundlegende regulatorische Anforderungen an Versicherungen kennen und vertraglich unterstützen?
- Welche Zertifizierungen wie ISO 27001 oder BSI C5 können Start-ups vorweisen, um die Erfüllung der Compliance-Anforderungen von Versicherungen zu erleichtern?
- Wie können Start-ups eine vertragliche Service-Erbringung nach deutschem Recht und in konfigurierbaren EU-Lokationen mit Einhaltung der EU-DSGVO ermöglichen und sich flexibel in die IT-Service Management-Prozesse von Versicherungen integrieren?
- Welche Maßnahmen sollten Start-ups ergreifen, um angemessene Verschlüsselung von in der Cloud gespeicherten Daten gemäß ihrem Schutzbedarf zu gewährleisten?
- Wie können Start-ups Flexibilität im Backup-Prozess sowohl in Bezug auf die Frequenz als auch den Speicherort bieten und sicherstellen, dass eine Datenlöschung unverzüglich erfolgt und in der Backupstrategie berücksichtigt wird?
- Welche Controls sollten Start-ups zur Absicherung von SaaS-Services zum "Stand der Technik" einsetzen, um die Daten angemessen zu schützen?
- Wie können Start-ups flexibel sein bei der Einbindung von Identitäten, Berechtigungen und Authentifizierungsverfahren auf Basis von Industriestandards, um den Bedürfnissen von Versicherungen gerecht zu werden?

Versicherungsunternehmen können sich beispielsweise mit folgenden Fragen auseinandersetzen:

- Wie kann die Wesentlichkeit der Ausgliederung bei der Nutzung von Services von Start-ups bestimmt werden?
- Welche Schritte müssen durchgeführt werden, um Risiken zu bewerten und technisch-organisatorische Maßnahmen für den Einsatz der Start-up-Lösung abzuleiten?
- Wie können Versicherungen eine umfassende Leistungsbeschreibung erstellen, um klare Erwartungen an das Start-up festzulegen und Service Level Agreements zu definieren?
- Wie können Versicherer sicherstellen, dass sie bei SaaS-Verträgen die regulatorischen Anforderungen sowie resultierende Rechte und Pflichten an das Start-up weitergeben können?
- Wie können Versicherungen eine Exit-Strategie entwickeln, um auch im Falle von Insolvenz oder Beendigung des Vertragsverhältnisses mit dem Start-up handlungsfähig zu bleiben?
- Wie kann im Fall eines Exits die "Daten-Übergabe" and einen weiteren Dienstleister sichergestellt werden?
- Wie können Versicherungen sicherstellen, dass ihre Daten im Falle der Löschung unverzüglich und vollständig gelöscht werden, einschließlich der Daten in den Backups beim SaaS-Partner?

HANDLUNGSEMPFEHLUNGEN FÜR VERSICHERER UND START-UPS

HANDLUNGSEMPFEHLUNG 1: Es sollte eine klare Definition der Rollen auf beiden Seiten vorgenommen werden, sowohl im Start-up als auch im Versicherungsunternehmen. Dabei sollten Fachlichkeit, Vertragsmanagement, Techniklösung, Service Management und kommerzielle Betrachtungen berücksichtigt werden. Es ist wichtig, dass jeder Rolle spezifische Aufgaben und Verantwortlichkeiten zugewiesen werden, um sicherzustellen, dass alle relevanten Aspekte der Zusammenarbeit abgedeckt werden.

HANDLUNGSEMPFEHLUNG 2: Es sollten klare und transparente Rahmenbedingungen für die Zusammenarbeit geschaffen werden. Dies beinhaltet Organisationsstrukturen, Verantwortlichkeiten, Service Level Agreements (SLAs), Statement of Work (SoW), Aufstellung eines "Steering Committee" und weitere relevante Aspekte. Durch eine klare Definition der Rahmenbedingungen von Anfang an können potenzielle Missverständnisse vermieden und ein reibungsloser Ablauf der Zusammenarbeit gewährleistet werden.

HANDLUNGSEMPFEHLUNG 3: Es sollte frühzeitig mit der Erstellung und Abstimmung von Compliance-Dokumenten begonnen werden, in enger Zusammenarbeit mit den beteiligten Stakeholdern. Dabei sollten die regulatorischen Anforderungen identifiziert und dokumentiert werden, um technisch-organisatorische Maßnahmen abzuleiten, die erforderlich sind, um diese Anforderungen zu erfüllen. Eine kontinuierliche Kommunikation und Abstimmung mit den Stakeholdern ist dabei von großer Bedeutung, um sicherzustellen, dass alle Anforderungen angemessen berücksichtigt werden. Dafür sollte gegebenenfalls ein Prozess geschaffen werden, der die Interessen von IT-Compliance-, Risikomanagement- und die Datenschutzfunktion sowie weitere notwendige IT-Governance-Funktionen sicherstellt.

HANDLUNGS-

HANDLUNGSEMPFEHLUNG 4: Es ist wichtig, dass das Unternehmen einen klaren Anforderungskatalog für SaaS-Dienste definiert hat, der aus regulatorischen Vorgaben und dem Schutzbedarf der Daten abgeleitet ist. Dadurch wird eine gezielte Auswahl und Bewertung von Start-up-Lösungen ermöglicht, um sicherzustellen, dass sie den erforderlichen Sicherheits- und Compliance-Standards entsprechen.

HANDLUNGSEMPFEHLUNG 5: Es sollte eine ausgewogene Lösung zwischen den "Must-Have"-Anforderungen aus der Regulatorik und der Risikoakzeptanz des Unternehmens gefunden werden. Dabei sollten die Compliance-Ziele erreicht werden, ohne dabei die Geschäftsziele und Innovationsfähigkeit des Unternehmens zu beeinträchtigen. Eine sorgfältige Abwägung und Priorisierung der Anforderungen sind hierbei von entscheidender Bedeutung.

HANDLUNGSEMPFEHLUNG 6: Die Rolle und Nutzbarkeit von Zertifikaten zur Absicherung der Regulatorik im Unternehmen sollte geklärt werden. Es sollte geprüft werden, ob bereits vorhandene Zertifikate genutzt werden können oder ob weitere Zertifikate erworben werden müssen, um bereits Standardcontrols zu erfüllen. Die Nutzung von Zertifikaten kann dazu beitragen, die Sicherheits- und Compliance-Anforderungen effizienter zu erfüllen und das Vertrauen in die Lösung zu stärken.

EMPFEHLUNG

3 BETRIEB

Während Start-ups sich oft zunächst auf die Entwicklung neuer Funktionalität konzentrieren, müssen für den IT-Betrieb mit der Einführung von Cloud-Nutzung weiterreichende Fragen belastbar geklärt werden. Diese sind nicht vollumfänglich durch das jeweilige Start-up zu beantworten, jedoch sollten diese sich dieser Aufgabenstellungen bewusst sein, um ihren Beitrag und ihre Beteilung klar darstellen zu können. Der Fokus liegt hier auf Betriebsqualität, Sicherheit und Effizienz.

Beim Einsatz einer (durch ein Start-up) entwickelten Cloud-basierten Lösung stellt sich für das VU die Frage, wie wesentliche Aspekte für den IT-Betrieb gelöst werden sollen, z. B.:

- die Sicherstellung einer SLA (Service Level Agreement) basierten 24/7 Betriebsbetreuung,
- die Einbindung in Backup, Monitoring und Incident Management,
- die Integration in ein (vielleicht noch nicht durchgängig etabliertes) DevSecOps Modell.

Weiterführende Aufgabenstellungen ergeben sich aus

- der Diskussion von zu DevOps passenden Arbeitszeitmodellen,
- der Berücksichtigung von externen Services in Business Continuity und K-Fall Planung,
- der Einbindung in unternehmensweites Change-Management und Security-Vorgaben,
- sowie dem Einsatz von IAM (Identity and Access Management) Systemen mit Rollen- und Berechtigungskonzepten.

VU werden eine neue SaaS-Lösung auch aus Sicht des Lizenzmanagements betrachten: Flexibilität, Nutzung eigener Lizenzen, Auditierbarkeit, Support, Laufzeiten und Verbindlichkeiten.

Für Start-ups wie für VU gleichermaßen interessant ist die Fragestellung nach einem passenden Liefer- und Bereitstellungsmodell – die Abwägung zwischen (managed) SaaS mit allen regulatorischen Implikationen (DSGVO etc.) und einem Softwarepaket zum Selbstbetrieb.

Zusammenfassend müssen sich Start-ups mit dem Gedanken beschäftigen, dass sie nicht nur eine fachlich überzeugende Lösung liefern, sondern auch Bausteine und Antworten für die wesentlichen Aufgaben eines Betriebskonzepts parat haben müssen.

4 IT-SECURITY

Das Thema IT-Sicherheit ist als Bestandteil der Informationssicherheit im Kontext von Cloud Computing bei der Zusammenarbeit von Start-ups und VU hochrelevant. Wie bereits in Kapitel 2 "Regulatorik" thematisiert, wird das Ziel verfolgt, sensible Informationen zu schützen. Dafür sollen so genannte Schutzziele eingehalten werden. Diese Schutzziele stellen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Authentizität der betreffenden Informationen dar. Um sie einzuhalten, können sowohl das VU als auch das Start-up bestimmte Schutzmaßnahmen ergreifen. Diese Maßnahmen lassen sich in technische und organisatorische Maßnahmen unterteilen.

Um Verzögerungen in der vertraglichen Anbahnung zu vermeiden und eine gemeinsame Grundlage für sicherheitsrelevante Aspekte zu schaffen, ist unsere Empfehlung, frühzeitig den Kontakt zwischen Start-up und IT Security des VU herzustellen.

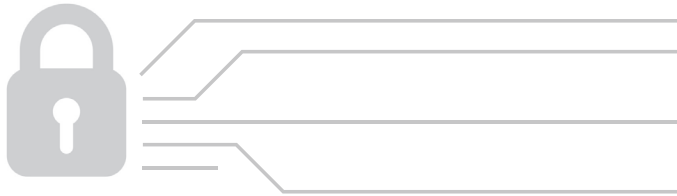
Für Start-ups lohnt sich die Orientierung an den Inhalten wesentlicher Richtlinien, z.B. ISO 27001, BSI C5, ISO 27018.

Wichtige Themenfelder sind:

- Verschlüsselung
- Datensicherung
- Business Continuity Management (BCM)
- Authentifizierung
- Autorisierung
- Firewalls

Für die strukturierte Erfassung / Aufbereitung / Bearbeitung möglicher Anforderungen empfiehlt sich die Orientierung an einem der gängigen Frameworks, z. B. dem NIST-Security Framework.

Der Austausch von Daten zwischen VU und Start-ups sollte durch geeignete technische und organisatorische Maßnahmen abgesichert werden, je nach Sensibilität der Informationen. Einen Anhaltspunkt für geeignete Maßnahmen bietet z. B. das Dokument "Stand der Technik" hier. Resilienz und Security neuer Lösungen werden von VU in Abhängigkeit von der Kritikalität u. a. auf Möglichkeiten zur eigenständigen Auditierung von Providern, Verfügbarkeit, Nutzung von Verfügbarkeitszonen und Regionen sowie Schutz der Daten vor Cyber- / Cryptoangriffen geprüft werden - darauf können sich Start-ups vorab vorbereiten.



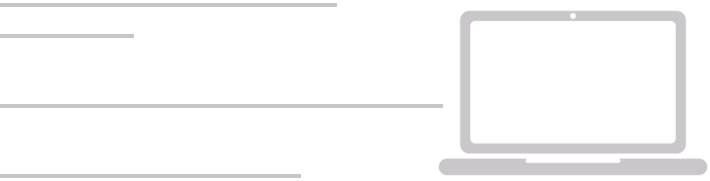
Im Bereich der Controls für Cloudeinsatz sind für VU folgende Aspekte wichtig für den Einsatz neuer Lösungen:

- Einbindung in Monitoring und Key Management sowie konsistentes IAM über On Prem & Cloud hinweg
- Standorte von Rechenzentren in Bezug auf Verfügbarkeit (Geo-Redundanz) von Services, Netzwerklatenz, Kosten
- Besondere Herausforderungen bei Multicloud-Ansätzen mit Providern auf jeweils verschiedenem Security bzw. Zertifizierungsleveln
- Aktuelle Trends, u. a. Application-aware Software-Defined-Network und Routing Lösungen, in denen Start-ups verstärkt aktiv sind

Besonderes Augenmerk sollte auf die Auswahl von Standorten im Geltungsbereich DSGVO / GDPR gelegt werden. Alternativ kann dies auch mittels Vertragsgestaltungen geschehen, die über den Einbezug der Standardvertragsklauseln der Europäischen Kommission oder einen Angemessenheitsbeschluss ein adäquates Schutzniveau bieten.

→ EU Model Clause

→ Ergänzung Angemessenheitsbeschluss



5 KULTUR & MINDSET

Vor dem Hintergrund einer frisch startenden Kollaboration zwischen VU und Start-up mit dem Ziel, neue Cloud-Technologien zu nutzen, sind vier wesentliche Erfolgsfaktoren zu nennen:

- Verständnis für die sehr unterschiedlichen Ausgangslagen bei Unternehmens- und Arbeitskultur sowie für die Entscheidungsprozesse der Unternehmen
- Verständnis für die sehr unterschiedlichen Mindsets der einzelnen handelnden Personen
- Klares Bekenntnis zu Anpassungsbedarf auf beiden Seiten, um den gemeinsamen Erfolg zu erzielen
- Pflege einer offenen "gemeinsam-Lernen-Kultur"

In einem (bislang eher traditionell aufgestellten) VU sind von einer Entscheidung für eine Cloud-Lösung deutlich mehr handelnde Personen betroffen und sollten frühzeitig einbezogen werden. Die Transparenz über die benötigten Rollen und Zuständigkeiten im Unternehmen stellt eine Herausforderung für Start-ups da, um effizient in einen produktiven Dialog mit einem VU einzutreten.

Das Mindset einer professionellen IT eines VU ist notwendigerweise von anderen Faktoren (Risiko, Regulatorik, Security, Betriebsqualität) geprägt als das eines Start-ups.

Eine klar identifizierbare Herausforderung auf Seiten der VU sind die individuellen Widerstände und Blockaden bei der Einführung von Cloud-Technologien. Ein darauf ausgerichtetes Schulungs- und Change Programm unterstützt den größeren Transformationsprozess im Unternehmen. Für die Start-ups bedeutet dies, dass sie erstmal verstehen müssen, in welcher Phase ihrer Transformation ein potentieller Kunde / VU sich befindet.

Eine gute Vorbereitung auf den Einsatz von Cloud-Technologien beinhaltet neben Schulungen zu Cloud auch fortlaufendes Cultural-Change-Training, um Motivation und Rollenwandel für die Mitarbeiter und Mitarbeiterinnen zu transportieren. Die besonderen Herausforderungen für VU im Bereich Security, Compliance, Risikomanagement aus den Kapiteln 2 bis 4 sollten allen Mitarbeitern und Mitarbeiterinnen transparent gemacht werden.

Nachhaltiger Erfolg bei der unternehmensweiten Nutzung von Cloud-Technologien bedarf eines aktiven Umgangs mit der Zukunft - Erhalt der Innovationsfähigkeit, andauerndes Lernen und stetiger Wandel durch zunehmende Change Geschwindigkeit auf den Technologie Stacks, Tools und Betriebsprozessen.

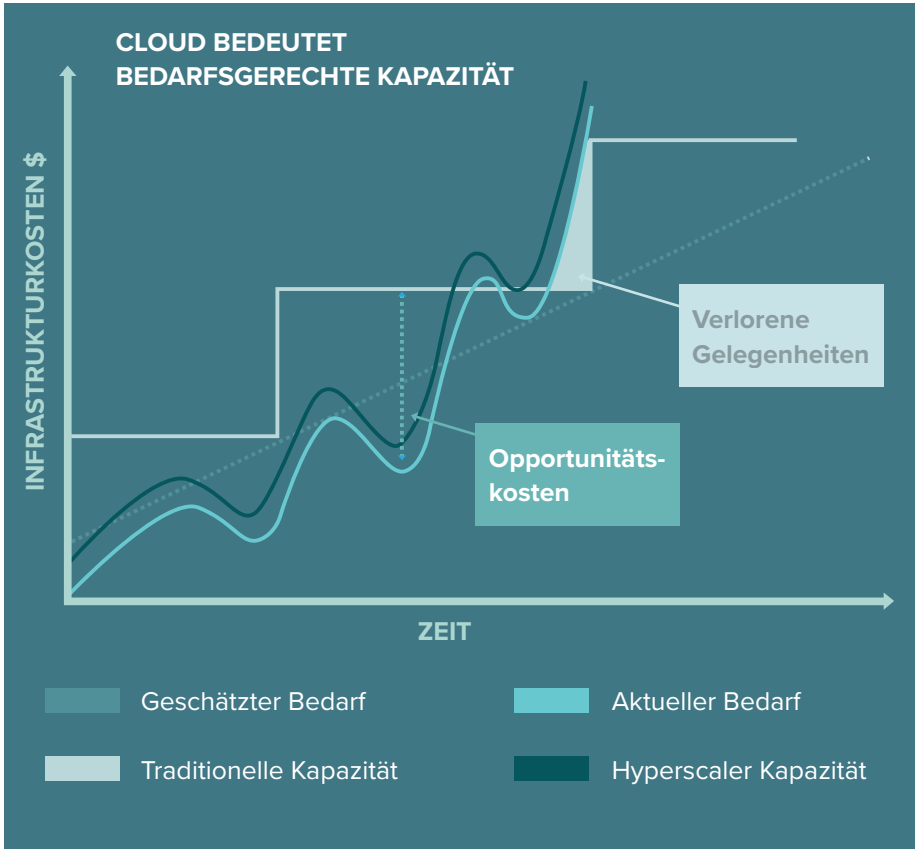
VGL DAZU DAS INSURLAB GERMANY WHITEPAPER "NEW WORK"

HIER DOWNLOADEN

6 BUSINESS CASE & KOSTEN

Die Bewertung eines Business Cases für neue Applikationen auf Cloud-Basis ist aus Sicht des VU sowie des Start-ups durchzuführen. Je nach Ausgangssituation des VU zählen unterschiedlich viele Elemente zur Betrachtung eines "einzelnen" Business Cases dazu - und alles, was die neue Lösung nicht mitbringt oder unterstützt, kann im Einzelfall schwer wiegen.

Die grundsätzliche Wirtschaftlichkeit der Cloud lässt sich am besten anhand eines Blickes auf die Infrastrukturkostenebene (SaaS vor PaaS vor IaaS) nachvollziehen. Durch die flexible Nutzungsmöglichkeit (pay-as-you-go-pricing) und nicht notwendige Anfangsinvestitionen (z. B. in Server) lässt sich die benötigte Kapazität sehr einfach an den tatsächlich vorhandenen Bedarf anpassen. Und zwar nicht nur im Falle von Mehrbedarf, sondern auch im Falle von Minderbedarf.



Quelle: Auszug aus AWS

Für die Start-ups, die tendenziell eher SaaS Lösungen entwickeln wollen, kann sich der Aufwand für zusätzliche Flexibilität bei Deployment und Betriebsverantwortung lohnen, um auch solche VU als Kunden zu gewinnen, die noch nicht voll handlungsfähig bei der externen Cloud-Nutzung sind.
Diese Flexibilität kann den Start-ups auch Zeit erkaufen, die Reife ihrer Lösung (sei es SaaS oder anders) voranzutreiben.

***7Rs: Sieben Strategien für Cloud-Migrationen:**

- Relocate
- Rehosting
- Replatforming
- Repurchasing
- Refactoring
- Retire
- Retain/move)

Tabelle mit dem Fokus: Zusammenspiel Start-up und VU

	Kernfragen für Versicherer (Cloud-Transformation)	**Kernfragen für Versicherer** (Einsatz SaaS-Lösung von Start-ups)	**Kernfragen für Start-ups** (Bereitstellung/ Betrieb SaaS)
Ausgangslage & Motivation	Business Case für SaaS vs Business Case für vollständige Public-Cloud-Transformation	Motivation verstehen - sind Kosten der einzige Grund für einen Cloud Einsatz? Wie passt meine InsurTech- (SaaS) Lösung in die strategische Ausrichtung der Transformation meines Versicherungskunden? Welche Rückwirkungen ergeben sich aus der Cloud-Nutzung auf das Unternehmen (organisatorisch)? Welche Kosteneffekte entstehen hierdurch? Bin ich mir als VU im Klaren, welche Facetten ich bei SaaS-Diensten berücksichtigen muss?	Ist meine Start-up SaaS-Lösung ein für das VU kritischer Teilprozess? Wo stehen meine Kunden und Kundinnen beim Einsatz von Cloud Technologie in ihrem Unternehmen? Welche Flexibilität erwartet das VU von der neuen SaaS-Lösung - kommerziell, betrieblich, technisch?

Einflussmöglichkeiten auf den BC durch verschiedene Parameter

Kernfragen für Versicherer (Cloud-Transformation)

- Welche "Hebel" gibt es für meinen Business Case Cloud für eine Anwendung?
- Welche Parameter beziehe ich in die Business Case Betrachtung ein (TCO)
- Wie kann der TCO (Total Cost of Ownership) abgeschätzt werden?

Kernfragen für Versicherer (Einsatz SaaS-Lösung von Start-ups)

- Was sind die Stellhebel für das VU für den Business Case?

Kernfragen für Start-ups (Bereitstellung/ Betrieb SaaS)

- Implementierungskosten und Betriebskosten für den Versicherer in Bezug auf das jeweilige Betriebsmodell (IaaS, PaaS, SaaS) ausrechnen. Eventuell sind mehrere Varianten zu rechnen.
- Will ich die Cloud-Flexibilität an den Versicherungskunden weiterreichen oder flat anbieten?
- Welche Anforderungen für Cloud muss ich für meinen Kundenkreis noch zusätzlich implementieren? Welche Hebel / Mehrwerte bietet mir der Cloud-Service / Produkt? Was kann die Versicherung abschalten?
- Wie sieht das Kostenmodell aus? (Lizenz oder / und nach Verbrauch)
- Welche Flexibilität kann ich bei der Laufzeit anbieten?
- Kenne ich die Kostentreiber meines SaaS-Dienstes?
- Optionen für weitere Anforderungen der VU.

	Kernfragen für Versicherer (Cloud-Transformation)	**Kernfragen für Versicherer** (Einsatz SaaS-Lösung von Start-ups)	**Kernfragen für Start-ups** (Bereitstellung/ Betrieb SaaS)
In welcher Phase befinde ich mich gerade	Wie komme ich zu einem kostenoptimierten Aufbau der Cloud-Lösung, wie zu einer kontinuierlichen Optimierung? Worauf muss ich bei verschiedenen Modellen (z. B. Single / Multi / Hybrid Cloud) achten?	Welche Effekte ergeben sich über verschiedene Phasen der Cloud-Nutzung?	Wie weit ist das Start-up in einem Cloud-Betrieb? Vgl. Kapitel 3. Wie weit ist das Start-up in der Entwicklung von Cloud- (nativen) Applikationen? Auswirkung auf Training, Entwicklungszeit und Lieferfähigkeit Welche Art von Verträgen können wir schließen? PoC, Implementierung, DL, ... Wie sieht das Kostenmodell im Blick auf verschiedene SLA-Level / Support aus?
Cloud-Modell/ Migrations-Modell	Wie gehe ich mit bestehenden Workloads / Applikationen um (Portfolio Management – 7Rs*)? Wie bewerte ich im BC potentielle neue Technologien / Möglichkeiten, die mir ohne Cloud nicht zur Verfügung stehen - jedoch nicht direkt auf diesen BC einzahlen?	Was muss ich als VU noch aufbauen, um die SaaS Applikation betreiben zu können? Wie schnell wäre die Lösung nutzbar?	Will ich nur Cloud-Lösungen anbieten oder auch Varianten, die On-Prem installierbar sind - quasi als Zwischenweg? Welche Cloud oder Multi Cloud bietet das Start-up an? Z.B. Hyperscaler, Telekom, lokale Player? Flexibles Deployment
Kostenmodell	Wie stelle ich Kostentransparenz sicher? Will ich das? Was ist Cloud Financial Management?	Wie können die Kosten des SaaS-Services in der Cloud effektiv verwaltet / getrackt werden?	Kann ich die laufenden Kosten korrekt vorhersagen und überprüfen? Wie gehe ich mit Abweichungen um? Wie skaliert mein Kostenmodell?

INSURLAB GERMANY

Hohenzollerring 85-87
50672 Köln
Tel.: +49 221 98 65 29 0

REDAKTION

INSURLAB GERMANY
connect@insurlab-germany.com

GRAFIK

JONAS GRAFIKDESIGN
+ 49 171 97 50 34 5
info@jonasstreit.de
www.jonasstreit.de