



Fakultät Informatik

**Analyse des "Vendor-Lock-In"-Risikos bei
führenden Cloud-Computing-Anbietern
unter Berücksichtigung der
Besonderheiten im GKV-Markt am
Beispiel der kubus IT eGbR**

Bachelorarbeit im Studiengang Medieninformatik

vorgelegt von

Ben Kretschmer

Matrikelnummer 3680674

Erstgutachter: Prof. Dr. Michael Zapf

Zweitgutachter: Prof. Dr. Uwe Wienkop

© 2026

Dieses Werk einschließlich seiner Teile ist **urheberrechtlich geschützt**. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Autors unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Einspeicherung und Verarbeitung in elektronischen Systemen.

Kurzdarstellung

Diese Arbeit ist in Zusammenarbeit zwischen dem IT-Dienstleister kubus IT und der Technischen Hochschule Georg Simon Ohm Nürnberg entstanden.

In dieser Arbeit wurde die These untersucht, ob sich die Anbieter für Cloud-Computing signifikant in dem Risiko für Vendor-Lockin unterscheiden.

Dazu wurde zunächst ein Katalog mit technischen Bewertungskriterien aufgestellt.

Anschließend wird definiert was technische Kriterien im Kontext von Cloud-Computing-Anbietern sind und diese werden gesammelt.

Auf Grundlage dessen werden mehrere Bewertungs-Modelle erstellt, die verschiedene Teilmengen des Kataloges einbeziehen.

Die Modelle werden im daraufhin gegen eine Auswahl diverser Anbieter getestet.

Zuletzt werden die Ergebnisse überprüft, indem die errechneten Ergebnisse mit den Einschätzungen der Cloud-Experten aus der kubus IT gegenübergestellt werden.

Inhaltsverzeichnis

1. Einleitung	1
1.1. Heranführung	1
1.1.1. Einleitung in das Cloud Computing	1
1.1.2. Cloud als Produkt	2
1.1.3. Überblick über die Nachteile der Cloud	2
1.1.4. Grundlagen der Anbieterbindung	3
1.1.5. Anbieterbindung in niedrigeren Liefermodellen	3
1.2. Motivation	3
1.2.1. Generelle Gründe für die Beschäftigung mit Anbieterbindung	3
1.2.2. Beenden von Anbieterbeziehungen	4
1.3. Abgrenzungen	4
1.3.1. Definition von technischen Kriterien	4
1.3.2. Distanzierung von ökonomischen Ansätzen	5
1.3.3. Auswahl der Cloud-Computing-Anbietern	5
2. Problemstellung	7
2.1. Ausgangssituation	7
2.1.1. Besonderheiten am Beispiel kubus IT	7
2.1.2. Resultierende rechtliche Vorschriften	7
2.1.3. Cloud-Architektur in der kubus IT	10
2.1.4. Vendor-Management in der kubus IT	11
2.2. Anforderungen	11
2.2.1. Zielsetzung der Analyse	11
2.2.2. Verifizierbarkeit der Ergebnisse	12
3. Lösungsansatz	15
3.1. Scoringmodell	15
3.1.1. Definition des Lösungsansatzes	15
3.1.2. Entwicklung von Bewertungskategorien	15
3.1.3. Kategorien mit indirektem Einfluss	16
3.1.4. Kategorien mit direktem Einfluss	17
3.1.5. Umgang mit Gewichtung	17
3.2. Alternative Ansätze	18
3.2.1. Gesetzliche Lösungen für Anbieterbindung	18

3.2.2. tbd2	19
4. Experimente	21
4.1. Modell-Prüfung	21
4.1.1. Intuitive Gewichtung	21
4.1.2. Faire Gewichtung	21
4.1.3. Gegenprüfung durch zufällige Gewichtung	21
4.2. Interpretation	21
4.2.1. Bedeutung der Ergebnisse	21
4.2.2. Aussagekraft des Modells	21
5. Ausblick	23
5.1. Handlungsempfehlung	23
5.1.1. tbd	23
5.2. Implementierung	23
5.2.1. tbd	23
A. Supplemental Information	25
Abbildungsverzeichnis	27
Tabellenverzeichnis	29
List of Listings	31
Literaturverzeichnis	33
Glossar	35

Kapitel 1.

Einleitung

1.1. Heranführung

1.1.1. Einleitung in das Cloud Computing

Das Schlagwort Cloud fällt sowohl im Heim-IT-Umfeld als auch in den Besprechungen und Büros der großen deutschen und internationalen Unternehmen regelmäßig. Es ist zusammen mit der künstlichen Intelligenz einer der wohl schillerndsten und meistverwendetsten Begriffe in der IT-Branche wie Thorsten Hennrich in seinem Fachbuch zu Cloud Computing nach der Datenschutzverordnung einleitend feststellte. [Hen, 2023]

Weniger eindrucksvoll klingt die ISO Norm, nach der Cloud Computing ein Paradigma, um einen netzwerkbasierten Zugang auf ein skalierbares und elastisches Reservoir gemeinsam nutzbarer physischer oder virtueller Ressourcen nach dem Selbstbedienungsprinzip und bedarfsgerechter Administration zu ermöglichen. [ISO, 2023]

Diese übersetzte Definition jedoch gibt einen Einblick in das vermeintliche Potential der Technologie. Zu den Vorzügen zählen daher Kosteneinsparung, verbesserte Skalierbarkeit, Wiederherstellungsmöglichkeiten, Datensicherheit und weitere Punkte, die im Kapitel 1.4 namens utopische Versprechungen des Cloud Computings im Buch Cloud Governance aufgeführt werden. [Mez, 2023]

Mit der Popularität ist klar, dass diese Vorteile schon beim Auflisten verlockend sind. Zudem lassen sich Vorteile wie der Kostenpunkt leicht quantifizieren und damit vergleichen. Auch die Skalierbarkeit lässt sich durch die Zeit messen, die es benötigt zusätzliche Hardware einzubinden, wenn beispielsweise hoher Verkehr es fordert. Ferner lassen sich auch andere Eigenschaften der verschiedenen Cloud-Produkte wie die Anzahl der Backups oder die Anzahl von Datenlecks gegenüberstellen.

1.1.2. Cloud als Produkt

Aus dem Konzept der Cloud wird durch die Anbieter ein Produkt oder ein Katalog mit Produkten. Der Bedarf nach den Leistungsversprechungen der Cloud ist enorm. Nicht nur das Trainieren, sondern auch das Nutzen von KI-Modellen auf der eigenen Hardware ist rechenaufwändig. Auch andere Anwendungen wie das Management von Kunden und Unternehmensressourcen wird immer komplexer.

Es gibt viele verschiedene Konfigurationen der Cloud.

Wie auch bei eigenen Rechenzentren aus einer Vielzahl von Architekturen und Marken gewählt werden kann, so gibt es bei der Wahl der Cloud Liefermodelle und Produktbausteine, die nach den Bedürfnissen des Kunden eingekauft werden können. Grundlegend kann gewählt werden wie viele Schichten des ursprünglichen Rechenzentrums in die Cloud gehoben werden sollen. Die entsprechenden Stufen hierzu sind ebenfalls in der ISO-Norm beschrieben und lauten (sortiert nach aufsteigender Kompetenzen des Anbieters):

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

[ISO, 2023]

1.1.3. Überblick über die Nachteile der Cloud

Die Herausforderungen und Nachteile der Cloud werden im späteren Kapitel 3.6 "Der organisatorische Einfluss von Cloud-Computing" des Buches "Cloud Governance" aufgelistet:

- Sicherheit (gegen Cyber-Angriffe)
- Kosten(-regulierung)
- (Integration von) Alt-Anwendungen
- Ausfälle
- Anbieterbindung
- (Verlust von) technischem Fachwissen

Die Aufzählung wurde aus dem Englischen übersetzt und es wurde Kontext ergänzt. [Mez, 2023] Die konkreten Punkte stammen aus einem Blog-Artikel der IT-Sicherheitsfirma Conosco. [Conosco, 2020] Der Fokus dieser Arbeit ist die Anbieterbindung. Eine tatsächliche Anbieterbindung ist nur auf der Ebene Software as a Service möglich.

1.1.4. Grundlagen der Anbieterbindung

Vendor-Lock-In (dt. Anbieterbindung) ist ein Umstand in der Beziehung zu einem Anbieter aus Kundensicht. Dieser Umstand wird beim Beenden der Beziehung problematisch. Denn möchte ein Unternehmen den Anbieter wechseln, so ist eine Anbitermigration nötig.

Grundsätzlich ist die Migration von einem Anbieter zu einem Konkurrenten immer mit Aufwand verbunden, wenn beispielsweise die Daten einer CRM-Anwendung des einen Anbieters zum Anderen gesendet werden müssen. Problematisch wird es dann, wenn die Daten in unterschiedlichen Formaten abgespeichert sind. Hilfreich sind dann Werkzeuge zur Migration, welche bei branchenüblichen CRM-Anwendungen leicht erhältlich sind. Waren beim ursprünglichen Anbieter jedoch Anbieter-eigene Lösungen im Einsatz, steigert sich der Migrationsaufwand über das zu erwartende Pensum hinaus.

Ein besonders schwerwiegender Vendor-Lock-In liegt vor, wenn Bausteine des Produkts gar nicht vom neuen Anbieter abgebildet werden können.

1.1.5. Anbieterbindung in niedrigeren Liefermodellen

In niedrigeren Liefermodellen wie Platform as a Service, wo die Anwendungen und Daten in der Hand des Kunden liegen, ist Anbieterbindung generell kein Problem. Dadurch, dass die Anwendungen bei allen Anbietern gleichermaßen durch den Kunden gewählt und betrieben werden, können diese Anwendungen zum neuen Anbieter einfach migriert werden.

Dies ist ebenfalls aufwendig, vor allem wenn die Umgebung beim neuen Anbieter anders ist. Jedoch ist eine Migration pauschal immer möglich.

Die Kunden haben dazu das technische Fachwissen im Hause, um die Anwendungen entsprechen zu modifizieren oder umzukonfigurieren, damit diese in der neuen Umgebung funktionieren.

1.2. Motivation

1.2.1. Generelle Gründe für die Beschäftigung mit Anbieterbindung

Die Beschäftigung mit Anbietern ist spannend, denn sie hat strategische und politische Komponenten. Die Wahl eines Cloud-Anbieters für ein Unternehmen ist elementar und Anbieterbeziehungen durchlaufen einen Lebenszyklus (vergleiche Software-Lebenszyklus). Obwohl es Diskrepanzen zwischen der Praxis und der Theorie gibt, so sollte schon bei der Schließung einer neuen Geschäftsbeziehung deren Ende und Wechsel-Strategie festgelegt

sein. Hierfür ist die Durchleuchtung eines Anbieters hinsichtlich Vendor-Lock-In schon im Voraus wichtig.

Da darüberhinaus die Anbieterbindung nicht während der Lebenszeit einer Anbieterbeziehung sondern am Ende ins Gewicht fällt, ist die Auseinandersetzung nicht so allgegenwärtig wie andere Cloud-Themen.

1.2.2. Beenden von Anbieterbeziehungen

Wie schon festgestellt, wird die Anbieterbindung beim Beenden einer Geschäftsbeziehung relevant. Dafür zentral ist, wann das Ende der Geschäftsbeziehung in einem Unternehmen erreicht ist. Bei alleinstehenden Anwendungen beispielsweise wird die Lebenszeit üblicherweise auf eine gewisse Jahreszahl begrenzt. Allerdings können wie auch bei den klassischen Anwendungen bei einem Cloud-Anbieter Bedingungen eintreffen, die einen früheren Wechsel verlangen.

Diese Bedingungen können finanzieller Art sein. So könnte etwa der aktuelle Anbieter in Anbetracht seiner Leistungen nicht mehr wirtschaftlich sein.

Nicht nur finanzielle Aspekte können zu einem Wechselwunsch beim Kunden führen.

Durch Anpassungen am Leistungskatalog und die vertragliche Möglichkeit manche Leistungen nicht mehr anzubieten, kann es dazu kommen, dass notwendige Bausteine nicht mehr vom Cloud-Computing-Anbieter unterstützt werden. Solche Anpassungen sind aufgrund der festen Vertragsregeln zwar nie plötzlich, meistens aber ein Argument für einen Wechsel.

Außerdem kann es dazu kommen, dass Kunden von mehreren Anbietern ihre benötigten Leistungen auf einen einzigen konsolidieren wollen oder im Gegenbeispiel ihre Anforderungen auf mehrere Anbieter verteilen wollen, um die unterschiedlichen Alleinstellungsmerkmale mehrerer Anbieter gleichzeitig zu nutzen.

Zuletzt kann es auch durch äußere Faktoren wie gesetzliche Vorgaben, denen das Produkt des aktuellen Anbieters nicht mehr folgt, dazu kommen, dass ein Wechsel unbedingt notwendig wird. Auch geopolitische Änderungen wie Zölle oder Gesetze zählen zu den Gründen für das frühzeitige Ende der Geschäftsbeziehung

1.3. Abgrenzungen

1.3.1. Definition von technischen Kriterien

Vendor-Lockin ist ein primär technisches Problem für den Käufer eines Produktes beziehungsweise konkret eines Cloud-Computing-Anbieters.

Daher wird untersucht welche technischen Kriterien zu diesem technischen Problem führen. Technische Kriterien sind Eigenschaften eines Produktes im Kontext von Cloud-Computing, die sich auf die inherente Struktur und die Bestandteile des Produktes beziehen.

1.3.2. Distanzierung von ökonomischen Ansätzen

Im Gegensatz dazu sind vertragliche oder ökonomische Kriterien Gegenstand dieser Arbeit. Zur Verdeutlichung wird also beispielsweise nicht untersucht, ob die These, dass das Nutzen eines teureren Cloud-Computing-Anbieter seltener zum Vendor-Lockin führt, zutrifft.

1.3.3. Auswahl der Cloud-Computing-Anbietern

Bei der Auswahl der Anbieter wurden sowohl solche berücksichtigt, die die kubus IT bereits verwendete, als auch solche die vermeintlich interessante Ergebnisse liefern sollten. Aktuell sind folgende Cloud-Computing-Anbieter bereits in Benutzung.

- Arvato
- Microsoft Azure

Darüberhinaus werden folgende Anbieter aufgrund ihrer Relevanz auf dem internationalen Markt, ihrer besonderen Größe oder ihrer Relevanz für deutsche Firmen berücksichtigt.

- Amazon Warehoue Services (Vereinigte Staaten)
- Google Cloud Plattform (Vereinigte Staaten)
- Alibaba Cloud (China)
- IONOS Cloud (Deutschland)

Kapitel 2.

Problemstellung

2.1. Ausgangssituation

2.1.1. Besonderheiten am Beispiel kubus IT

Die kubus IT ist durch ihre Funktion als Dienstleister für die gesetzlichen Krankenkassen AOK Bayern und AOK PLUS Teil der öffentlichen Verwaltung.

Die Krankenversicherungen dieser Institutionen zählen laut §4 des SGB V zu den gesetzlichen Krankenversicherungen. Daher werden neben versicherungsbezogenen Aspekten auch die informationstechnische Umsetzung im Gesetzestext und daraus abgeleiteten Organen geregelt.

2.1.2. Resultierende rechtliche Vorschriften

Durch die Arbeit für eine gesetzliche Krankenkasse ergeben sich Anforderungen bei der Wahl des Cloud-Anbieters.

Relevant sind Kapitel zehn bis zwölf des fünften Sozialgesetzbuches, wobei zum Teil auch Paragraphen vorheriger Kapitel referenziert werden. Grundlegend sind diese gesetzlichen Vorschriften nicht direkt bei der Frage der Anbieterbindung von Relevanz, sondern werden generell bei der Architektur der (Cloud-)Infrastruktur der gesetzlichen Krankenkasse wichtig.

Kapitel 10 - Buch V - Sozialgesetzbuch Das zehnte Kapitel des fünften Buches definiert Versicherungs- und Leistungsdaten, den Datenschutz und die Datentransparenz. Dieses Kapitel befasst sich mit Informationsmanagement. Ob die Informationen in digitaler Form oder in Form analoger Akten gespeichert sind ist hier nicht relevant. Stattdessen wird geregelt an wen die Daten weitergegeben oder durch wen die Daten verarbeitet werden dürfen.

Auch Fristen und Regeln zur Vernichtung der Informationen wird aufgeführt. Diese Regelungen bilden indirekt Anforderungen an das Informationssicherheitsmanagement und die Zugriffsmöglichkeiten auf Daten bei dem Cloud-Anbieter. [SGB, 2025a]

Kapitel 11 - Buch V - Sozialgesetzbuch Das elfte Kapitel des fünften Buches regelt alle Belange der sogenannten Telematikinfrastruktur. Laut dem §306 des selbigen Abschnitts handelt es sich bei der Telematikinfrastruktur um "die interoperable und kompatible Information-, Kommunikations- und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens sowie der Rehabilitation und der Pflege dient und [...]". [SGB, 2025b]

Folgen des Paragraph 307 In diesem Paragraphen werden datenschutzrechtliche Verantwortlichkeiten festgelegt (§307). Dieser Paragraph legt zusammengefasst fest, dass die Nutzer einer verteilten Infrastruktur, also beispielsweise die Nutzer eines Cloud-Anbieters, für eine rechtskonforme sichere Verarbeitung der schützenswerten Daten innerhalb des Netzes der verteilten Infrastruktur verantwortlich sind. Des Weiteren erstreckt sich die Verantwortlichkeit auch auf die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten. Der Nutzer ist dann nicht verantwortlich, wenn dieser nicht über die "Mittel der Datenverarbeitung mitentscheiden"[SGB, 2025b] kann, wie es in §307 lautet. Diese Regelung bedeutet im Kontext der Cloud, dass bereits beim Liefermodell Infrastructure-as-a-Service die Verantwortung zur rechtskonformen sicheren Verarbeitung beim Anbieter liegt, denn schon ab diesem Niveau wird die Mitsprache durch den Nutzer der Cloud über die Mittel der Datenverarbeitung eingeschränkt. Spätestens bei dem Liefermodell Software-as-a-Service, wo der gesamte Technologie-Stapel (einschließlich der Software) durch den Anbieter betrieben wird, liegt auch die Verantwortung vollständig bei diesem.

Folgen des Paragraph 308 In diesem Paragraphen wird der Vorrang von Schutzmaßnahmen vor der europäischen Datenschutz-Grundverordnung geregelt (§308). Zusammenfassend werden die "Rechte der betroffenen Person nach den Artikeln 12 bis 22 der Verordnung (EU) 2016/679 [...] ausgeschlossen, soweit diese Rechte [...] nicht oder nur unter Umgehung von Schutzmechanismen [...] gewährleistet werden können."[SGB, 2025b] Folglich muss ein Verantwortlicher einem Betroffenen Daten nicht aushändigen, wenn für die Aushändigung Sicherheitsmaßnahmen umgangen oder Daten ungesichert separat gespeichert werden müssten. Dieses Gesetz widerspricht also zunächst dem allgemeinen europäischen Recht, dass jederzeit die Daten eines Betroffenen beispielsweise für diesen offengelegt oder gelöscht werden müssen, wenn dieser das verlangt. Jene Regelung des §308 gilt allerdings auch nur dann, wenn die Datenverarbeitung rechtmäßig ist und beispielsweise die Einsichtnahme zweifelsohne nicht ohne Umgehung von Sicherheitsvorkehrungen möglich ist. [SGB, 2025b]

Für den Cloud-Anbieter bedeutet das, dass eine Schnittstelle zur Verfügung gestellt werden sollte, die eine geregelte Einsichtnahme in die Daten eines Betroffenen ermöglicht.

Kapitel 12 - Buch V - Sozialgesetzbuch Das zwölfte Kapitel beinhaltet unter anderem explizit den Einsatz von Cloud-Technologie im Gesundheitswesen in §393. Dort wird festgelegt, dass die Verarbeitung von Sozial- und Gesundheitsdaten im Weges des Cloud-Computing-Dienstes nur im Inland, einem Mitgliedsstaat der Europäischen Union oder einem der Mitgliedsstaat der europäischen Union gleichgestellten Staat wie der Schweiz und Mitgliedstaaten des europäischen Wirtschaftsraumes erfolgen darf. Alle anderen Staaten gelten als Drittstaaten müssen in einem sogenannten Angemessenheitsbeschluss für die Übermittlung personenbezogener Daten erst genehmigt werden. [SGB, 2025c]

Derzeit sind folgende Staaten als Drittstaat durch einen Angemessenheitsbeschluss zugelassen:

- Andorra
- Argentinien
- Kanada
- Färöer-Inseln (Bestandteil des Königreichs Dänemark) [Wikipedia-Autoren, 2026a]
- Guernsey (Im britischen Kronbesitz) [Wikipedia-Autoren, 2026b]
- Israel
- Isle of Man (Im autonomen britischen Kronbesitz) [Wikipedia-Autoren, 2026c]
- Japan
- Jersey
- Neuseeland
- Republik Korea (Südkorea)
- Schweiz
- Uruguay
- Vereinigtes Königreich
- Vereinigte Staaten von Amerika

[Hessen, 2025]

Darüberhinaus wird im Absatz 3 des §393 festgelegt, dass eine Verarbeitung nur zulässig ist, wenn technische und organisatorische Maßnahmen, die dem Stand der Technik entsprechen, zur Gewährleistung der Informationssicherheit ergriffen worden sind. Zudem muss ein Sicherheitszertifikat der datenverarbeitenden Stelle, also des Cloud-Anbieters, vorliegen und zusätzlich die Kriterien für Kunden, die im Prüfungsbericht des Testats enthalten sind, umgesetzt wurden. [SGB, 2025c]

Das geforderte Testat muss den Anbieter insofern zertifizieren, dass Sicherheitsvorkehrungen mit dem Niveau des C5-Typ2-Testats oder höher getroffen wurden.

Auf Basis dieser Gesetzte wird eine übergreifend gültige Strategie vom AOK Bundesverband veröffentlicht.

2.1.3. Cloud-Architektur in der kubus IT

Die Cloud-Architektur der kubus IT basiert auf den Vorgaben des AOK Bundesverbandes. Die kubus IT verwendet das Modell der hybriden und teilt den Bedarf für Cloud-Computing in zwei Bereiche.

Personenbezogene Daten in der Private Cloud Die Private Cloud ist eine Cloud-Umgebung, die nur einen bestimmten geschlossenen Nutzerkreis (z.B. Mitarbeitende eines Unternehmens) zur Verfügung steht." [Hen, 2023] Eine private Cloud-Umgebung nutzt dedizierte Infrastruktur was die Überwachung der Einhaltung der Gesetze zum Datenschutz erleichtert. Die Firma Arvato Systems ist der Cloud-Computing-Anbieter, der die private Cloud der AOK Bayern und AOK PLUS betreibt. Die Auslagerung des Betriebs der Infrastruktur ermöglicht hier einen Fokus und eine Spezialisierung auf beiden Seiten. So kann sich die kubus IT als IT-Dienstleister nach der Auslagerung auf den Betrieb der Anwendungen fokussieren.

Technische Daten in der Public Cloud Die Public Cloud ist eine Cloud-Umgebung, die von der Allgemeinheit also von jedermann genutzt werden kann." [Hen, 2023] Dennoch lassen sich die Daten und Dienste der Cloud durch Verschlüsselung und Authentifizierung sichern. Der Nachweis der Einhaltung der gesetzlichen Vorgaben zum Schutz personenbezogener Daten ist jedoch schwieriger. Die öffentliche Cloud beinhaltet stärker als die private Cloud die Skalierbarkeit und Agilität, die generell Cloud-Computing zugeschrieben wird. An dieser Stelle wird aus Leistungs-Perspektive von den großen Spielern des Cloud-Computing profitiert werden. Beispielsweise besonders deutlich wird das im Bereich der Entwicklung

neuer Anwendungen durch den Dienstleister kubus IT. Hier wird die Applikationen für Entwicklung und Betrieb von Microsoft verwendet (Microsoft Azure DevOps). Dieses Produkt ist unter Anderem so attraktiv, weil die Integration mit der Microsoft-eigenen Entwicklungsumgebung (IDE) ausgezeichnet ist. Außerdem bietet Azure DevOps viele Werkzeuge zur Umsetzung sauberer Entwicklungs- und Betriebsprozesse.

2.1.4. Vendor-Management in der kubus IT

Der Abteilung Einkauf ist die Abteilung Vendor-Management zur Orchestrierung der Beziehungen zwischen der kubus IT und Anbietern untergeordnet.

Die Anbieter werden in drei Kategorien segmentiert.

- A-Vendoren: Große Abhängigkeit, hohe Kritikalität und fehlende kurzfristige Austauschbarkeit
- B-Vendoren: Mittlere Vorlaufzeiten und Kosten für den Austausch
- C-Vendoren: Anbieter für Standardleistungen mit leichter Austauschbarkeit

Diese Anbieterkategorien sind nicht ausschließlich für Anbieter von Cloud-Computing konzipiert. Stattdessen wird bei jeder Geschäftsbeziehung im Vendoren-Management mit diesem Schema gearbeitet.

Demnach zählen folgende Anbieter aktuell in das A-Segment:

- Arvato: Cloud-Computing
- DATAGROUP: 'Install-Manage-Add-Change'-Dienstleister
- Avaya: Cloud-Kommunikation

2.2. Anforderungen

2.2.1. Zielsetzung der Analyse

Das Analyseverfahren soll einen Ausgabewert liefern, der beschreibt wie hoch das Risiko eines Vendor-Lock-Ins ist. Kurz der Faktor Vendor-Lock-In soll quantifiziert werden.

Damit lässt sich die dieser Punkt besser in künftigen Vergabeverfahren berücksichtigen, wo auch wirtschaftliche, strategische und inhaltliche Faktoren eine Rolle spielen.

Diese Riskobewertung wird zunächst als Prozentzahl angeben. Nachgelagert werden Bestimmungsgrenzen beziehungsweise Schranken zur Ablehnung oder Akzeptierung eines Anbieter diskutiert.

Die Gesamtbewertung des Risikos soll als Werkzeug zur fairen Gegenüberstellen verschiedener Anbieter dienen.

2.2.2. Verifizierbarkeit der Ergebnisse

Nachdem ein Prozess entwickelt wurde, der eine Bewertung des Vendor-Lock-In-Risikos liefert, muss im Anschluss diese Bewertung geprüft werden.

Vor der Entwicklung des Prozesses werden daher direkt Methoden der Verifikation vorgestellt. Die Verifizierbarkeit lässt sich durch drei Methoden abbilden. Es ist einerseits möglich die Bewertung des Modells mit der Einschätzung eines Experten im Cloud-Bereich zu vergleichen und andererseits bestehende Analysen als Messlatte zu wählen.

Darüberhinaus lassen sich die Ergebnisse auch durch das Messen des Aufwands der Migration testen. Eine Metrik für den Aufwand wäre die benötigte Arbeitszeit, die Kosten der Migration oder der Anteil der Anwendungen, die umgestellt werden müssen.

Um die durch das Bewertungsmodell vorgeschlagene Bewertung per Experiment zu überprüfen, muss der Aufwand Emigration vom Anbieter betrachtet werden. Doch auch das Ziel des gesamten Migrationsprozesses ist hierbei relevant und hat einen Einfluss auf den gesamten Aufwand. Generell werben Anbieter mit Angeboten und Werkzeugen, die bei der Migration unterstützen.

Damit die Experimente verschiedener Anbieter vergleichbar sind, sollte jedoch der Anteil des Aufwands, der auf die Immigration zurückzuführen ist, minimiert werden. Dazu zählt auch die Erleichterung der Migration durch eventuelle Dienstleistungen des Ziel-Anbieters.

Zur Bewerkstelligung hiervon kann die Immigration in ein niederes Liefermodell gewählt werden. So kann beispielsweise der Wechsel verschiedener Anbieter im Liefermodell Software-as-a-Service zu einem Anbieter mit dem Liefermodell Platform-as-a-Service betrachtet werden.

Obwohl der Trend zu umfangreicheren Liefermodellen geht und solche Migrationen generell eher aufwendig sind, hat diese Methode Relevanz, um die Bewertung der Anbieter generell zu überprüfen. Da solche Migrationen aufwendig sind, ist anzunehmen, dass die Aufwandsunterschiede der einzelnen Anbieter in Relation zum Gesamtaufwand niedrig sind.

Auch mit der Migration innerhalb eines Liefermodells kann experimentiert werden. Im Gegensatz zur vorherigen Methode ist anzunehmen, dass die Aufwandsunterschiede zwischen

Anbietern innerhalb eines Liefermodells in Relation zum Gesamtaufwand drastischer sind. Wichtig ist jedoch für einen fairen Vergleich, dass die Vendor-Lock-In-Risikobewertung vom Wechselziel besser ist als die beste Bewertung der zu untersuchenden Menge an Anbietern.

Der Grund für diese Einschränkung ist einerseits die Notwendigkeit einer Verbesserung, denn obwohl es beispielsweise wirtschaftliche Argumente für einen Anbieter mit einer höheren Anbieterbindung geben kann, ist im Kontext dieser Arbeit ein Wechsel in eine stärkere Anbieterbindung generell nicht sinnvoll. Andererseits sorgt eine bessere Bewertung implizit für eine höhere Kompatibilität zwischen zwei Anbietern.

Kapitel 3.

Lösungsansatz

3.1. Scoringmodell

3.1.1. Definition des Lösungsansatzes

Zur Ermittlung dieser Gesamtbewertung des Risikos wird ein gewichtetes Scoring-Modell entwickelt. Die inhaltlichen Kriterien des Modells können unabhängig von den jeweils dazugehörigen Gewichtungen definiert werden. Abhängig von den Ergebnissen der Verifizierungsphase können die Gewichte im Nachgang angepasst werden.

Je nach Fokus und Bedürfnissen des Anwenders können die einzelnen Kategorien auch durch Gewichtung priorisiert werden. Dadurch kann das breite Spektrum der Kategorien nach Bedarf reduziert werden.

3.1.2. Entwicklung von Bewertungskategorien

Die einzelnen Kriterien werden in Bewertungskategorien gegliedert. Grundsätzlich wurden die Kategorien durch die Ermittlung der Produktschnittmenge der Anbieter festgelegt:

- Amazon Azure

Darüberhinaus werden die Definitionen und Anforderungen folgender Stellen berücksichtigt:

- Gematik GmbH
- Sozialgesetzbuch

3.1.3. Kategorien mit indirektem Einfluss

Allgemein wird bei jedem Kriterium bewertet, ob der Cloud-Anbieter dieses Kriterium erfüllt. Die ungewichtete Punktzahl wird verdoppelt, wenn das Kriterium durch eine Standardlösung erfüllt wird, die nicht für den konkreten Anbieter einzigartig ist. Die Kategorie hat einen indirekten Einfluss auf die Anbieterbindung, wenn ein Kriterium oder konkretes Produkt Daten nutzt oder produziert, dessen Format umgewandelt werden muss oder die migriert werden müssen. Je mehr SaaS-Produkte ein direktes Pendant bei einem Ziel-Anbieter haben, desto schwächer ist die Anbieterbindung.

SaaS-Produkte für Tagesgeschäfte In dieser Bewertungskategorie wird der Anbieter auf seine Leistungen hinsichtlich Anwendungen für das Tagesgeschäft überprüft. Darunter zählen hier Anwendungen zur Pflege der Kundenbeziehungen oder der Unternehmensressourcen (CRM und ERP) Außerdem zählen Kommunikationsanwendungen in diese Kategorie.

SaaS-Produkte zur Datenspeicherung Es wird betrachtet welche Datenbank-Formate zum Einsatz kommen, um Daten des Unternehmens zu Speichern. Außerdem werden andere Speicherlösungen wie Blob-Speicher betrachtet.

Entwicklungs-Werzeuge Für Unternehmen, wie die kubus IT, in denen Anwendungen und Skripte für den eigenen Gebrauch innerhalb der Firma entwickelt werden, sind Werkzeuge zur Zusammenarbeit an Entwicklungsprojekten, zum Teilen und Speichern von Programmcode im Sinne einer Versionsverwaltung und zum effizienten Schreiben von Code im Sinne einer Entwicklungsumgebung notwendig.

Identitätenmanagement Das Konzept für Rechte, Rollen und deren Inhaber wächst üblich mit der Zeit und kann sehr komplex werden. Da es erstrebenswert ist, dass die Art und Weise wie Identitäten auf der Seite des Cloud-Anbieters funktionieren möglichst kompatibel mit anderen Lösungen ist, wird auch diese Kategorie im Katalog berücksichtigt.

Operationsstabilität SaaS-Produkte, die zur Stabilität im Betrieb beitragen, schützen beispielsweise die Infrastruktur vor Angriffen. Auch hier kann eine Migration notwendig werden, wenn beispielsweise Firewall-Einstellungen bei dem neuen Anbieter übernommen werden sollen.

Überwachung und Management [...]

Virtual-Desktop-Infrastruktur Betrifft Produkte eines Anbieters, die

3.1.4. Kategorien mit direktem Einfluss

Interoperabilität In dieser Kategorie werden Kriterien gesammelt, die zur generellen Interoperabilität beitragen und sich keiner anderen Kategorie unterordnen lassen. Unter Interoperabilität versteht man...

Das Konzept kann sowohl im Sinne der Zusammenarbeit zwischen mehreren aktiven Cloud-Anbietern innerhalb eines Unternehmen, der Zusammenarbeit von eigenen Rechenzentren und Cloud-Infrastruktur und auch im Sinne der Zusammenarbeit zwischen einem neuen und einem ehemaligen Anbieter verstanden werden. Diese Bereiche werden alle durch Kriterien dieser Kategorie abgedeckt.

Migrationswerkzeuge Werkzeuge zur Migration können als Werkzeuge, die beim Wechsel zu einem Anbieter hin oder von diesem weg, unterstützen verstanden werden. Darunter zählen zum Beispiel Anwendungen zum Export oder zum Versenden von gespeicherten Daten zu oder von einem anderen Anbieter.

Container-Lösungen Containerisierung unterstützt beim Betreiben von verschiedenen Anwendungen, indem diese Anwendungen in definierte Umgebungen gepackt werden. Es wird untersucht welche Containersierungstechnologien zum Einsatz kommen.

3.1.5. Umgang mit Gewichtung

Die Lösung ist so konzipiert, dass durch Feinjustierung der Gewichte, die Bedürfnisse des Anwenders berücksichtigt werden können. Initial sind jedoch folgende Gewichtungskonfigurationen vorgesehen.

Einheitliche Gewichtung Jedes Kriterium hat das gleiche Gewicht. Das Endergebniss hängt alleine von der Zahl der erfüllten Kriterien ab.

Schwerpunkt bei direkten Kriterien Viele erfüllte direkte Kriterien, bedeuten dass Aufwand eines Anbieterwechsels auf technischer Ebene erleichtert, denn es werden viele Hilfestellungen bei der Migration geboten. Um einen Schwerpunkt an dieser Stelle zu setzen, werden die Gewichte der Kriterien um einen gewissen Faktor erhöht. Alternativ kann das Bewertungsmodell auch so Konfiguriert werden, dass die übrigen Kriterien keine Gewichtung haben, wodurch die Gesamtbewertung ausschließlich direkte Kriterien beinhaltet.

Schwerpunkt bei indirekten Kriterien Sind viele indirekte Kriterien erfüllt, so lassen sich viele alte Anwendungen zu einem neuen Anbieter umziehen, weil die verwendeten Anwendungen nicht exklusiv für einen Anbieter sind. Das erleichtert die Migration der Anwendungsdaten, da die Daten nicht in das Format neuer Anwendungen übersetzt werden müssen. Außerdem ist eine solche Migration für die Mitarbeitenden weniger spürbar und diese müssen nicht in neue Software eingearbeitet werden. Daher haben auch die indirekten Kriterien eine große Relevanz. Analog zu dem vorherigen Paragraph, kann entweder eine alleinige Analyse oder schwerpunktmäßige Berücksichtigung durch eine entsprechende Konfiguration der Kriterien erfolgen.

3.2. Alternative Ansätze

3.2.1. Gesetzliche Lösungen für Anbieterbindung

Das Bewertungsmodell ist eine Lösung, die bei der Suche eines neuen Anbieters in einzelnen Unternehmen wie der kubus IT eingesetzt werden kann.

Schutz der Kunden vor Anbieterbindung Aus Sicht eines Cloud-Anbieters ist die Bindung seiner Kunden natürlich erstrebenswert. Und hat ein Anbieter im Vergleich zu den anderen Optionen auf dem Markt besonders attraktive und einzigartige Produkte, sodass der Kunde gar nicht wechseln kann, weil diesem sonst die Produkte fehlen, dann profitiert im gewissen Sinne auch der Kunde. Das ist jedoch nicht in erster Linie der Kern von Anbieterbindung. Vielmehr wird durch gezielte Ausgestaltung der Produkte eine Abhängigkeit aufgebaut, sobald der Anbieter einmal gewählt ist, was dem Kunden nur schadet, da es diesen einschränkt. So könnte man ein Gesetz gegen Anbieterbindung rechtfertigen.

Gesetzliche Möglichkeiten Anbieterbindung gesetzlich zu vollständig verhindern ist schwierig, da eine viele Faktoren zu einer Anbieterbindung beitragen. Daher liegt es nahe konkret einzelne Faktoren zu minimieren. Das ginge beispielsweise durch eine Pflicht zur Interoperabilität. So müssten zwangsläufig Daten in universellen Formaten gespeichert werden, damit diese leichter in Anwendungen neuer Anbieter importiert werden können.

Aktuelle gesetzliche Lösung In der europäischen Union gilt seit dem 12. September 2025 der sogenannte Data Act. Dieser enthält unter anderem "Regeln und entsprechende Interoperabilitätsvorgaben, die es Kunden von Datenverarbeitungsdiensten erleichtern, zu einem anderen Datenverarbeitungsdienst zu wechseln oder verschiedene Datenverarbeitungsdienste parallel zu nutzen. Bei Datenverarbeitungsdiensten handelt es sich vor allem um Cloud-Dienste. [Bundesnetzagentur, 2026]"

Einordnung des Data Act Zum Zeitpunkt der Themenfindung für diese Arbeit, stand das Inkrafttreten des Data Act unmittelbar bevor. Trotzdem war eine gesetzliche Lösung für die Anbieterbindung zum Zeitpunkt der Verfassung unbekannt. Der Data Act regelt folgende „Mindestanforderungen an Verträge“:

- Wechselrecht
- Unterrichts- und Unterstützungspflichten
- Kündigungsfristen und Kompensation bei vorzeitiger Kündigung
- Konkretisierung des Wechselprozesses

[Cross, 2025] Darüber hinaus muss ein Anbieter auf seiner Website offenlegen welche Maßnahmen getroffen wurden, um den Zugriff auf in der EU gespeicherte nicht-personenbezogene Daten durch andere Staaten zu verhindern. [Parlament, 2023] Zuletzt werden Gebühren für die Unterstützung beim Wechsel des Cloud-Anbieters durch Artikel 29 des Data Act schrittweise verboten. [Parlament, 2023]

Kapitel 4.

Experimente

4.1. Modell-Prüfung

4.1.1. Intuitive Gewichtung

[...]

4.1.2. Faire Gewichtung

[...]

4.1.3. Gegenprüfung durch zufällige Gewichtung

[...]

4.2. Interpretation

4.2.1. Bedeutung der Ergebnisse

[...]

4.2.2. Aussagekraft des Modells

[...]

Kapitel 5.

Ausblick

5.1. Handlungsempfehlung

5.1.1. tbd

[...]

5.2. Implementierung

5.2.1. tbd

[...]

Anhang A.

Supplemental Information

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Das hier ist der zweite Absatz. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Und nun folgt – ob man es glaubt oder nicht – der dritte Absatz. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Nach diesem vierten Absatz beginnen wir eine neue Zählung. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Abbildungsverzeichnis

Tabellenverzeichnis

List of Listings

Literaturverzeichnis

- [Hen, 2023] (2023). *Cloud Computing nach der Datenschutz-Grundverordnung*. O'Reilly.
- [Mez, 2023] (2023). *Cloud Governnance*. De Gruyter.
- [ISO, 2023] (2023). *Information technolgoy - Cloud computing - Part 1: Vocabulary*. ISO/IEC.
- [SGB, 2025a] (2025a). *Spzialgesetzbuch - (SGB V) Fünftes Buch - Gesetzliche Krankenversicherungen*, Kapitel Zehntes Kapitel. Bundesministerium der Justiz und für Verbraucherschutz.
- [SGB, 2025b] (2025b). *Spzialgesetzbuch - (SGB V) Fünftes Buch - Gesetzliche Krankenversicherungen*, Kapitel Elftes Kapitel. Bundesministerium der Justiz und für Verbraucherschutz.
- [SGB, 2025c] (2025c). *Spzialgesetzbuch - (SGB V) Fünftes Buch - Gesetzliche Krankenversicherungen*, Kapitel Zwölftes Kapitel. Bundesministerium der Justiz und für Verbraucherschutz.
- [Bundesnetzagentur, 2026] Bundesnetzagentur (2026). Informationen und Hintergründe zum Data Act.
- [Conosco, 2020] Conosco (2020). Challenges of moving to the cloud.
- [Cross, 2025] Cross, S. (2025). Data Act - Cloud-Switching: Wie wirkt sich der Data Act auf Vertragsverhältnisse aus?
- [Hessen, 2025] Hessen, D. (2025). Angemessenheitsbeschlüsse der Europäischen Kommission.
- [Parlament, 2023] Parlament, E. (2023). REGULATION (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
- [Wikipedia-Autoren, 2026a] Wikipedia-Autoren (2026a). Färöer.
- [Wikipedia-Autoren, 2026b] Wikipedia-Autoren (2026b). Guernsey.
- [Wikipedia-Autoren, 2026c] Wikipedia-Autoren (2026c). Isle Of Man.

Glossar

library A suite of reusable code inside of a programming language for software development. i

shell Terminal of a Linux/Unix system for entering commands. i