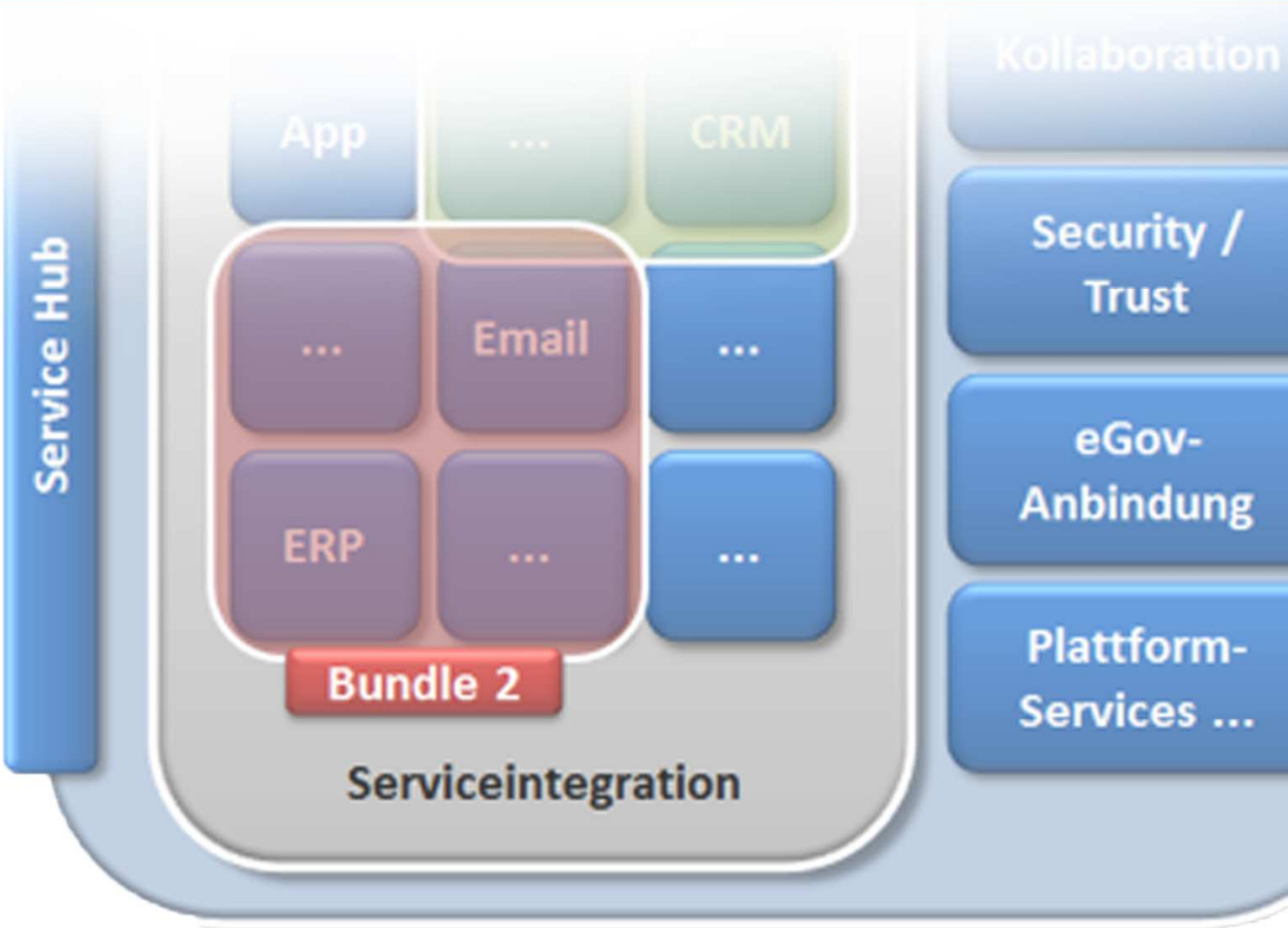
CLOUDwerker

AUFBAU UND BETRIEB EINER VERTRAUENSWÜRDIGEN, OFENEN DIENSTE-PLATTFORM FÜR DAS HANDWERK –

LEITFADEN FÜR DIENSTEANBIETER (SaaS Provider)



CAS SOFTWARE · haufe. · LEXWARE · 1&1 · Fraunhofer IAO · KIT Karlsruher Institut für Technologie · Forum Soziale Technikgestaltung · Handwerkstag BWHT · Trusted Cloud · Bundesministerium für Wirtschaft und Energie

CLOUDwerker

Aufbau und Betrieb einer vertrauenswürdigen, offenen Dienste-Plattform für das Handwerk – Leitfaden für Diensteanbieter (SaaS Provider)

Datum / Version: 2014-11-26 / V1.1

Dokumenten-Verantwortung: **AP3** Realisierung (unter Mitwirkung aller AP Partner)

Projektpartner:

CAS Software AG, Karlsruhe

1&1 Internet AG, Karlsruhe

Haufe-Lexware GmbH & Co. KG, Freiburg

KIT - Karlsruher Institut für Technologie, Karlsruhe

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart

Ansprechpartner:

Volker Jost

1&1 Internet AG

Ernst-Frey-Str. 9

76135 Karlsruhe

Telefon: +49 721 91374-0

E-Mail: volker.jost@1und1.de

1 Einführung

1.1 Motivation

Gerade kleine Handwerksunternehmen sind heute mehr denn je auf IT-Unterstützung angewiesen, um effizient typische Bürotätigkeiten und Aufträge abwickeln zu können. Auf Cloud-Technologien basierende Services haben dabei eine Reihe von Vorteilen: So entfällt der Aufwand für Installation, Gerätewartung, Datensicherung und Aktualisierung der Software. Doch nicht nur weniger Zeitaufwand und Kosten beim Betrieb dieser IT-Anwendungen, sondern auch neue Möglichkeiten, mit Geschäftspartnern und Kunden elektronisch über das Internet zusammenzuarbeiten, spielen in Zukunft eine immer wichtigere Rolle.

Im Rahmen des Projekts CLOUDwerker wurde eine Service-Plattform entwickelt, auf der Handwerker benötigte Dienste auf einer Plattform zusammenstellen und komfortabel buchen können. Für Softwaredienstleister bietet die Plattform die Möglichkeit, einzelne Services zur Verfügung zu stellen und mit komplementären Anbietern zu integrierten Dienstbündeln zusammenzufassen. Ein Mehrwertdienst kann dabei Dienste von einfachen Office-Anwendungen über Rechnungs- und Buchhaltungssoftware bis hin zu professionellen ERP- und CRM-Lösungen durchgängig kombinieren.

Dieser Leitfaden dient als Anleitung dazu, Unternehmen bei der Umsetzung von Service-Plattformen und der Bereitstellung von Dienstbündeln zur durchgängigen Bearbeitung von Geschäftsprozessen zu unterstützen. Grundlage hierfür bilden die Ergebnisse des CLOUDwerker-Projekts. Insbesondere wird dabei auf technische, wirtschaftliche und rechtliche Aspekte eingegangen.

Im Folgenden werden die Begriffe *Dienst* und *Service* synonymisch verwendet.

1.2 Zielgruppe und Aufbau des Leitfadens

Dieser Leitfaden richtet sich an

- **Infrastruktur-, Plattform- und Serviceanbieter**, die das Ziel verfolgen, eine offene, vertrauenswürdige Plattform sowie flexibel kombinierbare und durchgängig nutzbare Softwaredienste für bestimmte Zielbranchen im B2B-Umfeld bereitzustellen
- **Service Provider**, die Cloud-Infrastrukturen, Service-Plattformen und Marktplätze **technisch bereitstellen** oder betreiben
- **Serviceanbieter ohne Plattform**, die bereits über eigene Dienste verfügen und diese mit komplementäreren Diensten weiterer Anbieter zu sogenannten Mehrwertdiensten kombinieren und über eine Plattform zur Verfügung stellen wollen
- **Anbieter von On-Premise Lösungen**, die bisher nur über On-Premise-Lösungen verfügen, diese aber in Zukunft als SaaS anbieten möchten

Der Leitfaden ist so aufgebaut, dass in Kapitel 2 zunächst auf allgemeine Aspekte rund um die CLOUDwerker-Platform (CWP) eingegangen wird. Kapitel 3 beschreibt die Vorgehensweise zum Aufbau einer CWP, wobei hier auf Aspekte differenziert nach Zielgruppe eingegangen wird. In Kapitel 4 wird erläutert, wie eigene Dienste, Dienste von Partnern und Dienste Dritter in die Plattform integriert werden können. Erläuterungen zu Abkürzungen sind im Glossar zu finden, die zu Grunde gelegte Literatur ist im Literaturverzeichnis aufgeführt. Details zu den rechtlichen Rahmenbedingungen für Cloud-Diensteanbieter können dem Anhang entnommen werden.

2 Grundlagen

2.1 Dienstbündel und Plattform

In Abbildung 1 wird die Darstellung eines herkömmlichen Kabels genutzt, um ein paar Prinzipien von CLOUDwerker zu erläutern. Punkt 1 verweist auf den Kern, den Plattform Basisdienst. Er liefert den stabilen Unterbau für den Plattformbetrieb. Hier sind der Webserver und weitere Unterstützungsdienste wie der Verzeichnisdienst lokalisiert.

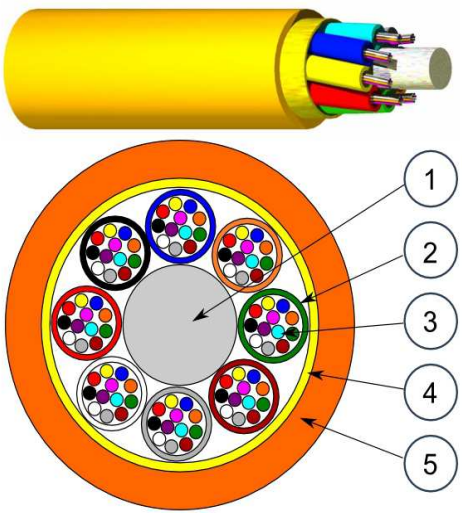


Abbildung 1 Dienstbündel und Plattform

Durch die mit Punkt 4 gekennzeichnet Schicht wird angedeutet, dass Dienstbündel (Punkt 2) in einem standardisierten Betriebsmodus an die Plattform gebunden werden. Je nach Anwendungsfall können aus den verfügbaren Dienste (Punkt 3) unterschiedliche Dienstbündel zusammengesetzt werden, die unabhängig voneinander auf der gleichen Plattform genutzt werden können. Hier bestimmt der Kontext die unterschiedliche Nutzung und verdeutlicht die Notwendigkeit von Mandantenfähigkeit der Dienste, also die Fähigkeit, auf derselben Plattform mehrere Kunden bzw. Auftraggeber zu bedienen, ohne dass diese gegenseitig Einblick in ihre Daten, Benutzerverwaltung und ähnliches haben.

Punkt 5 stellt die äußere Schutzschicht dar, die bei einem normalen Kabel die Fasern vor Beschädigung schützt. In dieser Schicht befinden sich, übertragen auf die (CWP) Verschlüsselungs- und Sicherheitsdienste, wie das einheitliche Nutzerzugriffsmanagement mit Funktionalitäten wie dem Single Sign On.

Abbildung 2 zeigt im übertragenen Sinne eine Bündelung von Diensten, verbunden mit erhöhtem Schutz; dennoch handelt es sich nur um eine klassische Dienstbündelung, wie wir sie heute auch von App Stores kennen: die Dienste untereinander sind inkompatibel. Jedoch soll die Schutzschicht die Dienstbündel nicht nur nach außen sicherheitstechnisch abschotten, sondern auch die Kommunikation zwischen den einzelnen Diensten und Dienstbündeln ermöglichen und somit dem Benutzer echten Mehrwert stiften.

Abbildung 2 klassische Dienstbündelung

Um den sicheren Datenaustausch zwischen verschieden Softwareapplikationen bis hin zu einem komplexen, kommunikativen Gesamtsystem aus unterschiedlichsten Diensten reibungslos zu garantieren, werden - eingebettet in eine Plattform - passende Schnittstellen und eine intelligentes Managementsystem benötigt. Dabei kann die Plattform Dienste anreichern, kontrollieren, ausbauen, kanalisieren, abrechnen, etc. All diese Aspekte sollen zentral in einer Trusted Cloud Plattform, hier am Beispiel der CWP, vereint werden.

Der Begriff des Plattformdienstes, wie er eben umrissen wurde, geht deutlich über den heute gebräuchlichen PaaS Begriff hinaus. Das im Rahmen von CLOUDwerker entwickelte Plattformkonzept ermöglicht, unter Berücksichtigung heutiger CLOUD Standards, die Integration und Orchestrierung von Softwarediensten unter gleichzeitiger Berücksichtigung hoher sicherheits- und datenschutztechnischer Standards.

2.2 Akkreditierung

Verbindliche Normierungen und Standards sind insbesondere im Cloud Computing notwendig. Nur so kann eine möglichst große Offenheit und Kompatibilität von Internetapplikationen und –diensten erreicht werden. Im Rahmen der Begleitforschung wurden Cloud-Standards untersucht, bewertet und ausgewählt. Die handwerksorientierte Plattform baut auf den gebräuchlichsten Protokollen und Standards auf. Dadurch können die Konzepte besonders gut umgesetzt und gleichzeitig Offenheit, sowie Erweiterbarkeit der Plattform aus technischer Sicht garantiert werden. Jedoch behält der Plattformbetreiber volle Handlungsfreiheit in der konkreten Ausgestaltung der Datenaustausche und Absicherung der Plattform. Wir empfehlen bei dem Aufbau einer Trusted Service Plattform auf Akkreditierungen (z.B. ECSA) der einzubindenden Dienste zu achten.

2.3 Cloud Computing Architekturen

Eine bekannte Gliederung von Cloud Computing Architekturen ist der sogenannte technische Cloud-Stack, der sich aus drei aufeinander aufbauenden Schichten zusammensetzt.

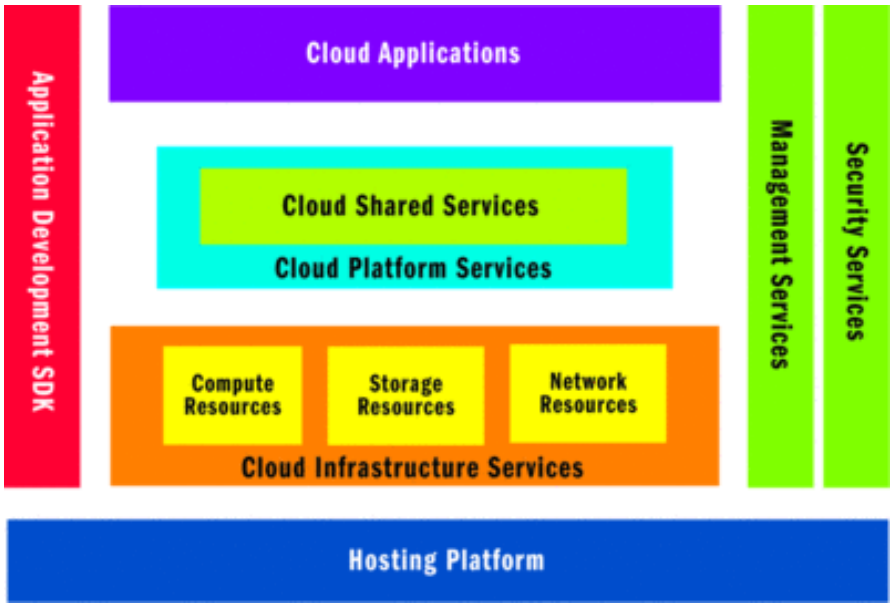


Abbildung 3 Beispiel für eine Cloud Architektur[1]

Hierbei wird unterschieden zwischen der ***Infrastruktur (Infrastructure as a Service, IaaS)***, der ***Plattform (Platform as a Service, PaaS)*** und dem ***Dienst (Software as a Service, SaaS)***.

- Infrastructure-as-a-Service (IaaS): Unter IaaS versteht man das bedarfsgerechte Vermieten von Rechnerinfrastrukturen. Bekannte Anbieter von IaaS sind Amazon (EC2 und S3), Google (Google Engine), IBM, HP, Microsoft oder T-Systems.

[1] http://msdn.microsoft.com/de-de/magazine/dd727504.aspx, Zugriff am 20.11.2014

- *Plattform-as-a-Service (PaaS):* Hierunter versteht man Laufzeit- und Entwicklungsumgebungen für Anwendungen, die in Cloud-Umgebungen laufen sollen. Der Plattform-Anbieter stellt Schnittstellen zu typischen Bausteinen der Anwendungsentwicklung, sowie eine Laufzeitumgebung zur Ausführung der Softwareapplikationen, zur Verfügung.
- *Software-as-a-Service (SaaS):* Anwendungen werden auf Plattformen und der dahinterstehenden Serverstruktur betrieben und im Browser des Anwenders angezeigt. Dieses Vorgehen hat den Vorteil, dass die Anwendung beim Anwender nicht lokal installiert werden muss, über offene Internet-Standards unabhängig von Plattform und Betriebssystem des Anwenders ist und dieser auch keine Wartung und Aktualisierung der Software durchführen muss.

Hier soll nicht tiefer auf Details von Cloud Architekturen eingegangen werden. Es sei vielmehr auf die vielen Definitionen von Herstellern[2], Online-Lexika[3] und Fachjournalismus verwiesen.

2.4 Trust und Sicherheit bei Cloud-Anwendungen

Der Schutz sensitiver Daten wie Auftragsinformationen, Adressen, Geschäftsprozesse und Bilanzen ist beim Betrieb von Mehrwertdiensten in Cloud-Umgebungen unerlässlich. Da Daten auch heute noch zum Teil unverschlüsselt in der Cloud abgelegt werden, ist den Anbietern der einzelnen Softwarekomponenten ausdrücklich zu raten, entsprechende Vorkehrungen zu treffen, die einen sicheren Umgang mit sensiblen Daten gewährleisten. Hierfür stehen heute schon eine Reihe automatisierter Tools zur Verfügung, die die Daten mit kryptographisch starken Algorithmen verschlüsseln. Hierbei sollte in der Initialisierungsphase ein asymmetrisches Verfahren wie RSA mit ausreichendem Sicherheitsniveau (>1024 Bit) verwendet werden. Die Verschlüsselung der Daten selbst geschieht dann mit einem symmetrischen Blockchiffreverfahren wie AES. Auch hier sollte ein ausreichendes Sicherheitsniveau (AES-256) gewählt werden. Die Kombination von asymmetrischen und symmetrischen Verfahren garantiert eine gute Performanz der Verschlüsselung, so dass Verfügbarkeit und Benutzbarkeit der Plattform durch die Verschlüsselung so wenig wie möglich beeinträchtigt werden. Algorithmen und Schlüssellängen sollten gemäß der aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder des National Institute of Standards and Technology (NIST) ausgewählt werden[4].

Um auch auf verschlüsselten Daten Funktionalitäten wie das Durchsuchen oder Sortieren der Daten oder die Verarbeitung von Datenbank- oder Tabellenbefehlen zu gewährleisten, ist eine einfache Volltextverschlüsselung nicht geeignet. Ein aktueller Ansatz des Forschungsprojektes MimoSecco zeigt, wie die Inhalte von Datenbanken geschützt werden können, die Datenbank aber nach wie vor durchsuchbar bleibt[5].

Wird die Ver- und Entschlüsselung der sensitiven Daten vom Cloudanbieter selbst durchgeführt, so empfiehlt sich die Verwendung einer *versiegelten* Cloud. Diese neu entwickelte Technologie schützt die Daten sogar vor dem Cloudanbieter, der die Daten verarbeitet[6].

[2] https://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf, Zugriff am 20.11.2014
[3] http://en.wikipedia.org/wiki/Cloud_computing, Zugriff am 20.11.2014
[4] http://www.keylength.com/
[5] http://www.mimosecco.de
[6] http://www.sealedcloud.de

2.5 Betreiberkonzepte & Geschäftsmodelle

Cloud-Konzepte

Im Hinblick auf Cloud-Services werden verschiedene Liefermodelle bzw. Organisationsformen unterschieden. Das Konzept einer Trusted Service Plattform ist auf alle diese Modelle gleichermaßen anwendbar, wobei sicherheitstechnische Anforderungen im Rahmen des Public Cloud Konzepts natürlich einfacher zu realisieren sind.

Public Cloud: Bietet Zugang zu IT-Infrastrukturen für die breite Öffentlichkeit über das Internet.

Private Cloud: Bietet Zugang zu IT-Infrastrukturen innerhalb der eigenen Organisation, meist via Intranet.

Hybrid Cloud: Je nach Bedürfnissen der Nutzer und den Anforderungen an Datensicherheit werden bestimmte Services durch externe IT-Infrastrukturen verarbeitet und andere Dienste intern abgewickelt.

Zentrale Architektur vs. verteilte Architektur

Im Hinblick auf Clouds unterscheidet man grundsätzlich zwei verschiedene Architekturen:

Zentrale Architektur: Alle Clients sind mit einem zentralen Server verbunden, der die komplette Zusammenarbeit abwickelt.

Verteilte Architektur/Peer-to-Peer-Architektur: Alle Clients sind über ein Netzwerk aus Servern verbunden; es gibt jedoch keine zentrale Verwaltungsinstanz.

Dieser Leitfaden widmet sich in erster Linie der Umsetzung einer Trusted Service Plattform mittels zentraler Architektur.

Geschäftsmodelle

Der Plattformanbieter ist ein Unternehmer, der eine zentrale Plattform für Cloud-Service Anbieter und Handwerker anbietet und vermarktet. Der Plattformanbieter kann auch gleichzeitig der Plattformhersteller sein, dies ist jedoch nicht zwingend notwendig. Das Geschäftsmodell betrachtet dabei aus Sicht eines Plattformanbieters zwei verschiedene Zielgruppen:

- **Cloud-Service Anbieter:** IT-Lösungsanbieter, die Cloud-Services über die Plattform für Handwerksunternehmen anbieten. Cloud Service Anbieter erhalten durch die Beteiligung an der Plattform einen Zugang zur Zielgruppe der Handwerker.
- **Handwerksunternehmen:** Endanwender der Cloud Services der CLOUDwerker-Plattform und damit die eigentlichen Nutzer der Services aus verschiedenen Branchen des Handwerks, z.B. Bauhaupt- und Ausbaugewerbe, gewerblicher Bedarf, KFZ-Gewerbe, Nahrungsmittelgewerbe, Gesundheitsgewerbe und personenbezogene Dienstleistungen.

Hinsichtlich der Zielgruppe der Cloud-Service Anbieter kann das Wertversprechen als „Bereitstellung einer handwerkerorientierten Plattform für Cloud-Services“ formuliert werden. Die Plattform bietet den Cloud-Service Anbietern eine Möglichkeit, die Zielgruppe der Handwerker zu erreichen und für die Nutzung ihrer Cloud-Services zu gewinnen, wobei den Cloud-Service Anbietern mit Hilfe einer technischen Rundum-Unterstützung seitens des Plattformanbieters der Zugang und die Teilnahme an der Plattform erleichtert werden soll.

Das Bezahlmodell für die Cloud-Service Anbieter kann wiederum verschiedenartig ausgestaltet sein. Eine Möglichkeit ist, dass Cloud-Service Anbieter einen einmaligen Aufnahme- bzw. Mitgliedsbeitrag entrichten. Eine zweite Variante stellt ein nutzer- bzw. volumenabhängiger Provisionssatz an den Plattformanbieter dar.

Für Plattformanbieter sind damit grundsätzlich zwei Geschäftsmodelle möglich, die sich vor allem in der Tiefe und dem Umfang der Bereitstellung einer Plattform unterscheiden.

"Full Stack": Der Plattformanbieter/-betreiber betreibt die auf seiner Plattform angebotenen Services auf seiner eigenen Infrastruktur, leistet Support, ist für das Billing zuständig, stellt zentrale, für alle Services verbindliche AGB und kontrolliert jede Applikation, deren Betrieb und Service Level. Dadurch erhält der Kunde ein Schlüssiges Gesamtkonzept und Services aus einer Hand.

"Flyweight": Der Plattformanbieter/-betreiber stellt nur ein minimales Service Bundle (Billing, Servicekatalog, Search) und setzt zudem nur einen Grundgerüst an allgemeinen "Richtlinien" (zu verwendende Schnittstellen, Protokolle usw.) auf.

Für den letztendlichen Erfolg des Geschäftsmodells ist insbesondere wichtig, dass der Plattformanbieter als vertrauenswürdig wahrgenommen wird. Dies ist Grundvoraussetzung, damit beide Zielgruppen an der Plattform teilnehmen. Eine vertrauenswürdige Plattform ist wiederum attraktiv für die Teilnahme durch Cloud-Service Anbieter.

2.6 Rechtliche Aspekte

Beim Aufbau einer CWP sind auch unterschiedliche rechtliche Aspekte zu berücksichtigen. Die Bewertung und die Umsetzung der rechtlichen Problemstellungen hängen maßgeblich von der Wahl des Geschäftsmodelles ab.

Je nachdem ob das grundsätzliche Modell „Full Stack“ oder „Flyweight“ gewählt wird, sind unterschiedliche rechtliche Implikationen in die Umsetzung einzubeziehen bzw. die unterschiedlichen Vor- und Nachteile in rechtlicher Hinsicht gegeneinander abzuwägen. Dabei ist auch zu berücksichtigen, dass die Erfüllung einzelner Rollen der beteiligten Plattformbetreiber bzw. Anbieter einzelner Diente und nicht nur bei einem einzigen Unternehmen liegen können, sondern unter Umständen auch auf Kooperationspartnerschaften verschiedener Unternehmen basieren.

Bei der Prüfung der beiden Modelle sind verschiedene Rechtsgebiete zu beachten, die – je nach Anwendung und Ausgestaltung – betroffen sind.

Im Rahmen eines CWP Projektes sind deshalb vor allem die nachfolgenden rechtlichen Implikationen zu berücksichtigen:

- Gesellschaftsrechtliche Gestaltung
- Telekommunikations- und Telemedienrecht
- Vertragsrechtliche Gestaltung
- Datenschutzrecht
- Datensicherheit
- Urheberrecht und Lizenzen
- Haftung

Zusammenfassend kann – je nach konkreter Umsetzung - festgestellt werden, dass das Modell „Full Stack“ zwar zunächst für die Handwerker den Vorteil bringt, nur einen Vertragspartner zu haben, der im Fall von technischen Problemen nicht nur Ansprechpartner, sondern eben auch rechtlich verantwortlicher für Support, Mängelbeseitigung bzw. etwaiger weitergehender Gewährleistungs- und Haftungsansprüche ist. Dies bringt für den Plattformbetreiber aber zugleich den Nachteil erheblicher rechtlicher Risiken für sämtliche angebotene Leistungen mit sich.

Das Modell „Flyweight“ hingegen gewährleistet eine klarere Abgrenzung der Verantwortungs- und Risikobereiche. Im Rahmen der entsprechenden vertraglichen Gestaltung kann und sollte der Plattformbetreiber gegenüber den Nutzern klar regeln, wer welche Leistungen erbringt bzw. wer im Falle von Mängeln und Schäden für entsprechende Gewährleistungs- oder Haftungsansprüche einzustehen hat.

Um im Rahmen des Modells „Flyweight“ dennoch eine „Trusted Cloud“ anbieten zu können, wird der Plattformbetreiber im Verhältnis zu den Diensteanbietern klare Vorgaben festlegen müssen, die als Anforderung zur Teilnahme an der Plattform Cloudwerker erfüllt werden müssen und ggf. nachzuweisen sind. Die fortgesetzte Einhaltung der Vorgaben könnte gegebenenfalls. vom Plattformbetreiber überwacht werden.

Eine ausführlichere Betrachtung ist im Anhang verfügbar.

Weiterführende Literatur:

Trusted Cloud Datenschutzrechtliche Lösungen für Cloud Computing – Thesenpapier der AG Rechtsrahmen des Cloud Computing[7]

Trusted Cloud, Vertragsgestaltung beim Cloud Computing – Thesenpapier der AG Rechtsrahmen des Cloud Computing[8]

Trusted Cloud, Lizenzierungsbedarf beim Cloud Computing – Thesenpapier der AG Rechtsrahmen des Cloud Computing[9]

Bundesamt für Sicherheit und Informationstechnik (BSI), Sicherheitsempfehlungen für Cloud Computing Anbieter[10]

[7] http://www.trusted-cloud.de/media/content/140228_Thesenpapier_Datenschutz_gesamt_RZ.pdf, Zugriff am 17.11.2014

[8] http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf , Zugriff am 17.11.2014

[9] http://www.trusted-cloud.de/media/content/140228_Arbeitspapier_Lizenzen_gesamt_RZ.pdf , Zugriff am 17.11.2014

[10] http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf, Zugriff am 17.11.2014

3 Aufbau der Plattform

Beim Aufbau der Plattform sind technische und nicht technische Aspekte zu berücksichtigen. Es geht also nicht nur um die Hardware, um Betriebssysteme und Techniken zur Virtualisierung sowie Nutzerfunktionalitäten, sondern auch um die Auswahl des Plattformkonzepts, die Planung/ Konzeption der Plattform und Komponenten, Dienste, Vorgehensweisen zur „Dienstbündelung“ und Wirtschaftlichkeitsrechnung. In diesem Zusammenhang soll nachfolgend auf relevante Fragestellungen eingegangen werden.

3.1 Wie wird man zum Betreiber einer Service Plattform?

Dieser Abschnitt richtet sich in erster Linie an Infrastruktur- und Serviceprovider, die bisher keine eigene Plattform betreiben und Interesse haben eine Trusted Service Plattform aufzubauen. Deshalb sollen hier zunächst kurz relevante technische Fragestellungen behandelt werden.

3.1.1 Wie wird eine CLOUDwerker Plattform aufgebaut?

Die Eigenschaften einer CWP bauen grundsätzlich auf denen gewöhnlicher Cloud Plattformen auf. Für eine geeignete CWP wurden vier Kriterien identifiziert: Die Bereitstellung von Basisfunktionalitäten, die Erweiterbarkeit, die Skalierbarkeit und die Offenheit. Diese Anforderungen werden bei CLOUDwerker wie folgt gelöst:

Bereitstellung der benötigten Basisfunktionalität

Damit komplexe Services auf der Plattform Hand in Hand arbeiten können, müssen bestimmte Basisdienste auf der Plattform bereitgestellt werden. So bilden beispielsweise ein gemeinsames Kundenverzeichnis, ein Dienste übergreifendes Kalendersystem und ein gemeinsames Dokumentarchiv die elementare Basis für das Zusammenspiel von Services wie CRM, ERP, usw.

Außerdem müssen zentrale Hintergrundfunktionalitäten wie eine Registry für die verfügbaren Dienste zur gemeinsame Authentifizierung und Autorisierung auf der Plattform realisiert werden.

Erweiterbarkeit

Die Plattform ist selbst ein lebendes Objekt, das anpassbar und erweiterbar sein soll. Ziel ist es, unterschiedlichste Softwareservices ohne großen Aufwand in die Plattform einzubinden. Um auf veränderte Marktbedingungen oder neue Technologietrends reagieren zu können, soll die Plattform auch für neuartige Anwendungsdienste offen und erweiterbar sein.

Die Architektur der Plattform soll so aufgebaut sein, dass beispielsweise neue Datentypen auf einfache Art und Weise ergänzt und existierende Schnittstellen (beispielsweise für CRUD-Operationen zum Lesen und Ändern von Daten) trotzdem unverändert weiterverwendet werden können.

Es soll auch möglich sein, Erweiterungen für Anwendungsdienste einfach zu integrieren. Denkbar ist z.B., dass als Erweiterung für das gemeinsam genutzte Kundenverzeichnis die Integration eines externen Adressbrokers zur Qualitätssicherung der Kundendaten eingebunden werden kann.

Um das Kriterium der Erweiterbarkeit zu erfüllen, sollte ausschließlich auf offene und breit genutzte Standards gebaut werden.

Skalierbarkeit / Ausfallsicherheit

Die Plattformarchitektur muss so ausgelegt sein, dass die zugrundeliegende Infrastruktur einfach erweitert werden und die Plattform mit der Anzahl der Nutzer wachsen kann. Zum Beispiel sollte es möglich sein, die Plattform bei wachsender Benutzerzahl durch simples Hinzuschalten weiterer Applikationsserver entsprechend mitwachsen zu lassen.

Durch das Vorhalten weiterer Applikationsserver kann flexibel auf den Ausfall einzelner Server reagiert werden.

Offenheit

Um von einer offenen Plattform sprechen zu können, sollten folgende Kriterien erfüllt sein:

- Leichter Zugang für Dritt-Anbieter, die ihre Dienste auf der Plattform anbieten möchten
- Verwendung offener und technologisch unabhängiger Standards, wie z.B. http, OAuth 2.0, etc.
- Breite Unterstützung verschiedener Technologien (Java, .Net, PHP, etc.)

3.1.2 Welche Dienste sollte die Plattform bereitstellen?

Die Dienste einer CLOUDwerker-Plattform können in zwei Gruppen eingeteilt werden:

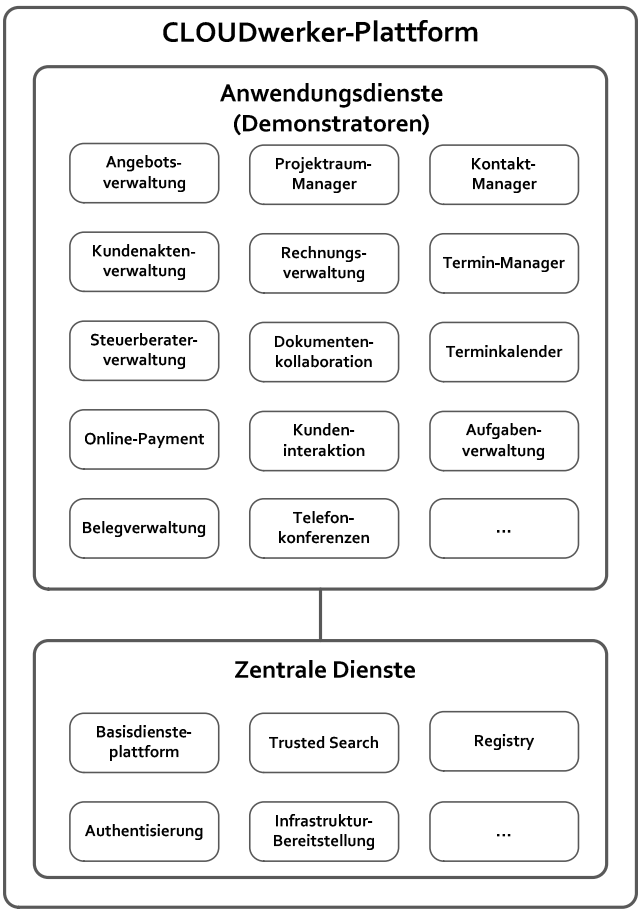


Abbildung 4: Komponenten der CLOUDwerker-Plattform

Die zentralen Dienste stellen elementare Funktionen bereit, die in aller Regel von allen Komponenten genutzt werden und im Hintergrund laufen:

- Registry mit Verzeichnis der verfügbaren Komponenten und Bündel
- Trusted Search zur Auswahl der für den Handwerker geeigneten Servicekomponenten oder Bundles
- Gemeinsames Nutzer-Verzeichnis
- Dienste zur Authentifizierung und Autorisierung
- Single Sign-On (SSO)

Die Anwendungsdienste, die von der Plattform zur Verfügung gestellt werden, umfassen die Verwaltung von typischen Stamm- und Groupware-Daten:

- Kontaktmanager
- Kundenaktenverwaltung
- Terminkalender / Termin-Manager
- Aufgabenverwaltung
- Angebotsverwaltung / Rechnungsverwaltung / Belegverwaltung

Zum anderen werden aber auch Basisfunktionen/-dienste für spezifische Anwendungen, wie z.B. für Kollaborationswerkzeuge, bereitgestellt:

- Projektraummanager
- Telefonkonferenzen
- Kundeninteraktion

oder für sonstige Spezialanwendungen:

- Dokumenten-Kollaboration
- Steuerberater-Verwaltung
- Online-Payment

Nicht alle Dienste, die im Rahmen von CLOUDwerker auf einer Plattform bereitgestellt wurden, sind auch zwingend erforderlich. Vielmehr hängt es vom Kontext, in dem eine Trusted Service Plattform aufgebaut werden soll, und insbesondere von den Komponenten/Diensten, die auf der Plattform genutzt werden sollen, ab, ob ein Dienst obligatorisch oder optional ist.

Im Rahmen von CLOUDwerker wurden alle genannten Dienste im Demonstrator umgesetzt. In der nachfolgenden Tabelle ist eine Abschätzung enthalten, welche der Dienste für vergleichbare Plattformen voraussichtlich obligatorisch und welche optional sind. Grundlage für diese Einordnung ist das Feedback aus den Evaluationen mit den im Projekt beteiligten Handwerksunternehmen.

Dienst	obligatorisch	optional
Zentrale Dienste		
Registry mit Verzeichnis der verfügbaren Komponenten und Bundles		x
Trusted Search zur Auswahl der für den Handwerker geeigneten Komponenten oder Bundles		x
Gemeinsames Nutzer-Verzeichnis	x	
Dienste zur Authentifizierung und Autorisierung	x	
Single Sign-On (SSO)		x
Billing, Abrechnungsdienste	x	
Monitoring, Überwachung, z.B. von SLA	x	
Anwendungsdienste		
Kontaktmanager	x	
Kundenaktenverwaltung	x	
Terminkalender / Termin-Manager	x	
Aufgabenverwaltung	x	
Angebotsverwaltung / Rechnungsverwaltung / Belegverwaltung	x	
Projektraummanager	x	
Telefonkonferenzen		x
Kundeninteraktion	x	
Steuerberater-Verwaltung		x
Dokumenten-Kollaboration	x	
Online-Payment		x

Tabelle 1: Dienstematrix

3.1.3 Welche sicherheitstechnischen Aspekte sind bei der technischen Spezifikation zu beachten?

3.1.3.1 Authentifizierung mit Single-Sign-On (1&1)

Empfohlene Standards:

- OpenID
- SAML2
- LDAP

Zur zentralen Authentifizierung nutzt die CWP den HIP[11] Single-Sign-On Service auf Basis von SAML2. Hierbei wird die Anfrage der Dienste zur Authentifizierung von Nutzern signiert, so dass sichergestellt ist, dass nur registrierte Dienste Nutzerinformationen bekommen. Zum anderen findet die Authentifizierung ausschließlich über HTTPS statt, so dass auch ein Ausspähen der Nutzerinformationen über den Kommunikationskanal nicht möglich ist.

[11] Host Identity Protocol

Der HIP Single-Sign-On Service wurde in der CWP als Identity Provider mit eigner Nutzerverwaltung auf Basis eines LDAP Systems aufgebaut. Er kann auch als Schnittstellen-Adapter eingesetzt werden, um Dienste über andere offene Standards und Protokolle zu authentifizieren.

Gerade bei der Anwender-Authentifizierung bietet der Einsatz von etablierten und weit verbreiteten Standards den Vorteil, dass recht einfach ein föderiertes, zentrales Identitätsmanagement aufgebaut werden kann.

Für die einzelnen Serviceprovider, die ihre Dienste auf der Plattform zur Verfügung stellen, hat dies zum Vorteil, dass sie keine eigene Benutzerverwaltung aufbauen müssen, sondern auf die zentrale Authentifizierung zurückgreifen können. Nur so kann auch für den Anwender ein Single-Sign-On über mehrere Dienste der Plattform hinweg realisiert werden.

3.1.3.2 Autorisierung der Zugriffe auf die Dienste

Zur Absicherung der Zugriffe auf die Dienste setzt die CWP auf den offenen Standard OAuth 2.0.

OAuth 2.0 baut konsequent auf bereits etablierte Standards wie z.B. HTTP, SSL auf. Dies trägt maßgeblich zum einfachen und trotzdem sehr sicheren Einsatz des Protokolls und letztendlich zu dessen weiten Verbreitung bei.

Dienste auf der CLOUDwerker Plattform, die dieses Protokoll nutzen möchten, müssen zu SSL verschlüsselten http-Abfragen fähig sein. Dies ist in beinahe jeder im Internet eingesetzten Programmiersprache möglich. Somit werden keine zusätzlichen Bibliotheken oder Frameworks benötigt, die evtl. nicht in allen Programmiersprachen zur Verfügung stehen.

Die CLOUDwerker Plattform bietet mit dem HIP Autorisationsservice „Authorization as a Service“ basierend auf OAuth 2.0 an. Hierbei wurde ein „rollenbasiertes Zugriffskontrollsystem“, ein „Role Based Access Control“ System entwickelt, bei dem der Zugriff auf HTTP Verben basierend definiert und Rollen zugeordnet werden kann. In Abb. 5 ist eine grafische Darstellung des RBAC-Systems zu sehen. Dabei werden die Daten von Clients (nicht im Sinne von Nutzern sondern Systemen), Rollen, und deren Beziehungen in unterschiedlichen Tabellen abgelegt und sind dort im Zusammenspiel von Befehlen und Funktionen als Kombinationen abfragbar, sodass konsistente Aussagen bzgl. der Zulässigkeit eines Zugriffs möglich sind.

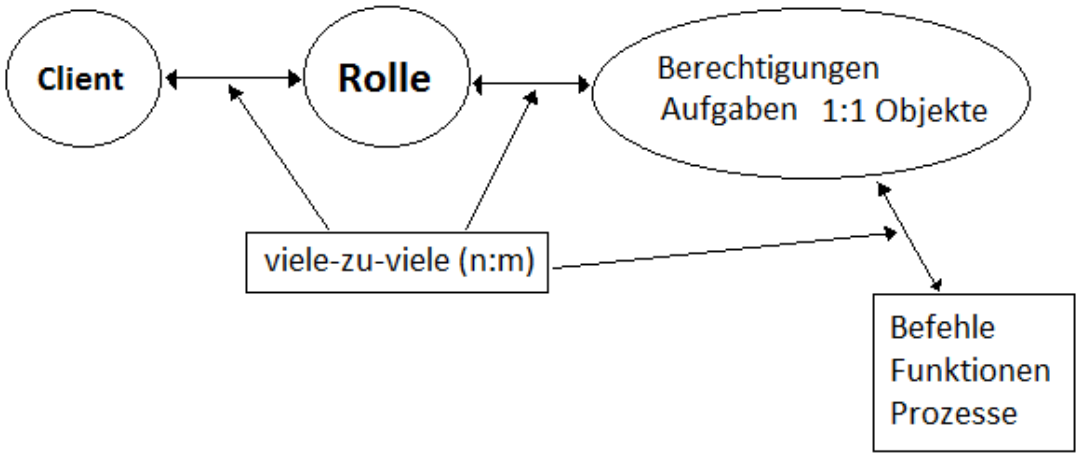


Abbildung 5 Prinzip des RBAC, des rollenbasierten Zugriffsmodell

Die HIP Registry nutzt z.B. den HIP Autorisationsservice, um das Lesen von Dienste-Endpunkte allen Clients zu erlauben, das Verändern eines Dienste-Endpunktes aber nur dem zugehörigen Dienst selbst.

3.1.3.3 Absicherung der Kommunikation (SSL / AES)

Zu Absicherung der Kommunikation zwischen den Diensten wird SSL mit AES Verschlüsslung eingesetzt. Auch die Kommunikation zwischen Benutzer und Plattform, insbesondere die Identifizierung über das HIP sollte über eine HTTPS-Verbindung erfolgen.

3.1.4 Wie arbeitet die Registry?

Die HIP Registry verwaltet alle Dienste der CLOUDwerker Plattform; also sowohl die Basisdienste der Plattform selbst, als auch Dienste von Dienstanbietern.

Über die HIP Registry können Dienste nach bestimmten Kriterien gesucht werden. Zur Charakterisierung der Dienste dient der USDL Standard.

USDL geht bei der Beschreibung über den rein technischen Aspekt, wie z.B. der Beschreibung der technischen Schnittstelle des Dienstes, hinaus und bietet die Möglichkeit, beispielsweise Nutzungskosten Funktionen usw. zu beschreiben.

Die HIP Registry unterstützt den „Hypermedia as the Engine of Application State“-Ansatz. D.h. die Registry dient zum Auffinden des zentralen Einsprung-Punktes eines Dienstes. Danach übermittelt der Dienst selbst per Hypermedia, welche Endpunkte aus welchem Zustand heraus aufgerufen werden können.

3.2 Wie wird eine Plattform zu einer Trusted Service Plattform?

Dieser Abschnitt soll sich insbesondere an Interessenten richten, die bereits über Plattformlösungen verfügen. Um den Schritt von der gewöhnlichen PaaS zur Trusted Service Plattform gehen zu können, müssen einige Kriterien rund um das Thema Vertrauenswürdigkeit berücksichtigt und umgesetzt werden.

Bevor große Umstrukturierungen und Arbeiten unternommen werden, sollten die existierenden Plattformdienste einer Anforderungsanalyse unterzogen werden und damit geprüft werden, inwiefern die Anforderungen von CLOUDwerker bereits erfüllt sind. Dabei sind Kriterien wie Transparenz, Compliance, Verantwortungsvoller Umgang mit Daten und Anpassbarkeit zu beachten

3.2.1 Vertrauenswürdigkeit

Dieser Abschnitt beschreibt die wesentlichen Faktoren, die aus Sicht eines Kunden die Vertrauenswürdigkeit einer Service Plattform determinieren. Zu jedem dieser Faktoren werden konkrete Empfehlungen und Beispiele zur Umsetzung genannt.

a) *Technische Sicherheit* (Verschlüsselung, Zugriffsschutz, Schutz vor Hacking)

   Technische Sicherheit bildet den Grundstein für eine Trusted Service Plattform. Es wird vom Plattformbetreiber erwartet, dass neueste Sicherheitsstandards und –Technologien eingesetzt werden.

Technische Sicherheit lässt sich am besten durch Zertifizierungen glaubhaft machen:

- Eigene Plattforminfrastruktur z.B. durch TÜV zertifizieren lassen
- Transparenter Onboarding / Audit Prozess für Dienste, die auf dieser Plattform laufen sollen. Wenn potentielle Kunden sehen, dass nur „zertifizierte Dienste“ auf der Plattform laufen und wenn es auf Wunsch einfach nachvollziehbar ist, welche Facetten eine solche Zertifizierung umfasst, so ist dies ein Qualitätsmerkmal

In Abschnitt 3.1.3 sind weitere Details und Umsetzungsempfehlungen zum Thema technische Sicherheit zu finden.

b) *Kontinuität in Betrieb und Weiterentwicklung*
Die Kernfrage an dieser Stelle ist: „Kann der Kunde darauf vertrauen, dass die Plattform dauerhaft weiterbesteht und weiterentwickelt wird?“

Diese Frage ist für Kunden einer Plattform sehr wichtig. Nur wenn sie daran glauben können, dass eine Plattform dauerhaft verfügbar ist, werden sie in den Migrationsaufwand hin zu dieser Plattform auf sich nehmen.
Der Track Record und die Nachvollziehbarkeit des dahinterstehenden Geschäftsmodells eines Plattformanbieters sind hier entscheidende Qualitätsmerkmale: Firmen wie Amazon, Apple oder Google wird ein Kunde glauben, dass deren Marktplätze bzw. Plattformen dauerhaft Bestand haben, weil diese (a) bereits lange existieren, (b) klar ersichtlich ist, wie die Betreiber damit ihr Geld verdienen und (c) gut glaubhaft ist, dass diese Marktplätze in die Unternehmensstrategie passen. Startups hingegen haben es hier schwerer: Wieso sollten Kunden Zeit und Geld in die Migration auf eine neue Serviceplattform investieren, wenn nicht ersichtlich ist, wie die nächste Finanzierungsrunde des Plattformbetreibers (Startup) dargestellt werden soll.
Als Plattformbetreiber ist es also wichtig, glaubhaft machen zu können, dass die Plattform dauerhaft betrieben werden soll. Zu den möglichen Maßnahmen gehören:

1) *Transparenz des Geschäftsmodells hinter der Plattform*:

   Beispiel: Ein Versprechen „dauerhaft kosten- und werbefrei“ löst bei Kunden die Frage aus, wie der Plattformbetrieb nachhaltig finanziert werden soll. Hier würde bereits die nicht glaubwürdige Nachhaltigkeit des Plattformbetriebs Kunden detrahieren, noch bevor sie über das Wertangebot „dauerhaft kostenfrei“ nachdenken.

2) *Offenlegung der Vision, Unternehmensstrategie und -historie:*

   Passt der Betrieb einer Plattform zur Unternehmensstrategie und kann das Unternehmen zudem auf Expertise und Historie in diesem Bereich verweisen, erhöht dies die Glaubwürdigkeit und kann helfen, den Kunden vom zukünftigen Erfolg des Unternehmens und dem Fortbestand der Plattform zu überzeugen.

c) *Kompetenz*:

Wie gut beherrschen Plattformbetreiber und Diensteanbieter der Plattform Ihre angebotenen Dienstleistungen?

In diesem Aspekt geht es vor allem um die Fähigkeit der Service- und Plattformbetreiber bzw. dessen Personal. Zu den Kernfragen gehören: Sind diese Unternehmen und deren Personal ausreichend geschult, um die Plattform und die Dienste einwandfrei zu betreiben? Was für Maßnahmen zur Qualitätssicherung werden ergriffen? Welche organisatorischen und technischen Datenschutzmaßnahmen gibt es? Wo lagern die Daten genau?

Die Kompetenz der Plattform- und Servicebetreiber lässt sich über deren Track Record und über transparente Darstellung der Maßnahmen zur Mitarbeiterqualifizierung und zur Qualitätssicherung nachweisen. Auch ein Sichtbarmachen der „Menschen" hinter den Plattformen und Diensten trägt aus Sicht der Kunden dazu bei, Vertrauen in die Kompetenz des Unternehmens zu schaffen, da sie dann auf einmal nicht mehr nur anonyme Services nutzen, sondern sehr wohl auch mit den Menschen dahinter interagieren.

d) *Compliance*:

Funktioniert der angebotene Dienst ordnungsgemäß?

Zu den zentrale Fragestellungen dieses Vertrauensaspekts gehören: Hält z.B. eine angebotene cloudbasierte Buchhaltung die rechtlich vorgeschriebenen Grundsätze ordnungsgemäßer Buchführung ein? Sind die angebotenen Services konform mit den geltenden Datenschutzvorgaben?

Auch hier sind Zertifikate ein geeignetes Mittel (z.B. GoBS Testat für einen Buchführungsdienst) für einen glaubwürdigen Nachweis. Auch der Hinweis auf eine Gesellschaftsform, die dem deutschen Recht unterliegt und damit auch dem deutschen Datenschutzgesetz, ist in diesem Zusammenhang bereits vertrauensbildend.

e) *Transparenz*:

Wie geht die Plattform mit kritischen Vorfällen (z.B. Störungen, Angriffen) um?

Hier ist die Außenkommunikation entscheidend: Wie geht der Betreiber z.B. mit einer ungeplanten Störung um? Transparenz und Aufrichtigkeit sind auch hier vertrauensbildend. Viele Betreiber von Onlinediensten veröffentlichen inzwischen automatisiert Status-Seiten, auf denen die Verfügbarkeit ihres Dienstangebots und die Störungen der letzten Zeit automatisch erfasst und aufgelistet werden (z.B. http://status.basecamp.com). Ziel dieser Seiten ist – neben Echtzeitinformation des aktuellen Dienst- / Plattformstatus – auch das glaubwürdige Belegen eines dem Kunden gegebenen Verfügbarkeitsversprechens (z.B. 99,9% versprochene Dienstverfügbarkeit wurde im Zeitabschnitt x tatsächlich erreicht).

f) *Datenhoheit / Lock-In*:

Wem gehören die Daten? Wie kann der Kunde seine Daten exportieren?

Zentrale Fragen dieses Aspekts sind: Werden beim Löschen des Kundenkontos die

zugehörigen Daten auch wirklich vom Server entfernt? Was passiert mit den Daten, wenn der Plattformdienst gekündigt wird?

Besonders in diesem Punkt sollte sich eine Trusted Service Plattform von gewöhnlichen Cloud-Lösungen abheben. Um von vornherein das Vertrauen der Kunden zu gewinnen, steht verantwortungsvoller und transparenter Umgang mit Daten an erster Stelle. Aus diesem Grund sollte ein Kunde bereits bei der Registrierung oder während einer kostenlosen Testphase verstehen, was bei einem potenziellen Ausstieg aus dem Dienst bzw. der Plattform passiert: Wenn ein Kunde von vornherein weiß, dass er alle Daten später wieder exportieren kann, startet er mit größerem Grundvertrauen in die Nutzung einer neuen Plattform, als wenn die Plattform eine Daten-Einbahnstraße ist. Dies gilt sowohl für die Plattform selbst, als auch für die darauf angebotenen Dienste.

Der Kunde sollte also jederzeit die Möglichkeit haben, seine Daten in gängige Datenaustauschformate (z.B. CSV) zu exportieren, oder komplett von der Plattform zu löschen. Um einen solchen Standard auch konsistent für Dienste von Drittanbietern, die auf der Plattform angeboten werden, zu garantieren, sollte ein Plattformbetreiber entsprechende Richtlinien und Regeln etablieren, die bereits beim Onboarding neuer Dienstanbieter in die Plattform dafür sorgen, dass o.a. Export- und Löschfunktionen in einem Mindestumfang von jedem einzelnen Dienst zur Verfügung gestellt werden.

Ein weiterer Schritt in diese Richtung wäre die Anforderung des Plattformbetreibers an jeden einzelnen Dienst auf der Plattform, eine spezielle Schnittstelle der Plattform zu implementieren, über die ein Kunde zentral für all seine abonnierten Dienste einen Datenexport oder Löschung veranlassen kann. Als technisches Beispiel hierfür sei das Google Konto erwähnt: Über diese Funktion kann ein Nutzer zentral all seine abonnierten Google und Nicht-Google Dienste verwalten, alle Daten aller Dienste exportieren und zentral all seine Daten löschen.

3.2.2 Dienstbeschreibung und Richtlinien für externe Dienste

Die Beschreibung der Dienste ist zentraler Baustein der Trusted Service Plattform. Nur so können Dienste entsprechend der Kundenanforderungen ausgewählt und gebucht werden. Über grundlegende Informationen wie Kosten, Anbieter etc. hinaus, sollte die Dienstebeschreibung einfache Service Level Agreements beinhalten.

Neben Tutorials und Hinweisen zur sicheren bzw. korrekten Nutzung der Dienste können Testversionen dazu benutzt werden, dem Kunden ein Gefühl für den Dienst und seine Leistungsumfänge zu geben.

Darüber hinaus ist es wichtig für angebotene Dienste, insbesondere von Drittanbietern, klare und einheitliche Richtlinien und Rahmenbedingungen zu schaffen. Dies soll vor allem zur Sicherung der Qualität in Sachen Datenschutz bzw. Vertrauenswürdigkeit dienen und dabei helfen, eine stimmige Produktauswahl anzubieten.

3.2.3 Bedarfsgerechte Service-Auswahl

Abb. 6 zeigt einen, in drei Phasen untergliederten, Prozess für die Auswahl und Einführung von Cloud Diensten durch einen Handwerker. Die ersten beiden Phasen beinhalten Schritte für eine bedarfsgerechte Service-Auswahl und reichen von der Ermittlung der fachlichen und nicht-fachlichen

Anforderungen, bis hin zur Auswahl geeigneter Dienste oder Service-Bündel. Die dritte Phase beinhaltet die Bereitstellung und Konfiguration eines gewählten Cloud Dienstes, den Test sowie die Übernahme in die Nutzung dieses Dienstes bzw. Service-Bündels durch den Handwerker. Dieser Prozess ist die Grundlage für den ebenfalls, im CLOUDwerker-Projekt, entstandenen Leitfaden für die Auswahl und Einführung von Cloud Diensten für Handwerker [Christm2014].

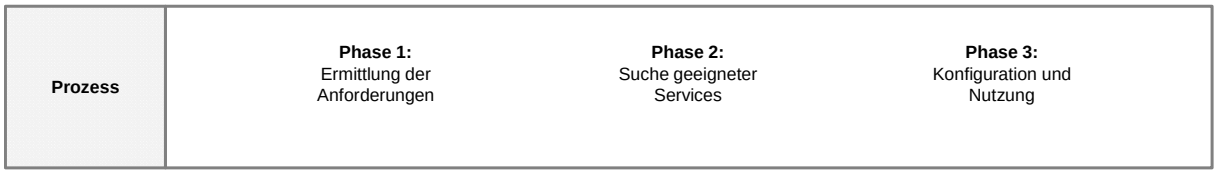


Abbildung 6: Prozess für die Auswahl und Einführung von Cloud Dienste durch einen Handwerker

Diese Prozesskette kann durch die Anbindung eines Trusted Service Finder (TSF) an eine CLOUDwerker-Plattform optional unterstützt werden. Ein TSF ist ein web-basiertes Werkzeug, das eine bedarfsgerechte Service-Auswahl für Handwerker auf der Grundlage eines vereinfachten Verfahrens ermöglicht. Dabei hat ein TSF seinen Schwerpunkt auf den ersten beiden Phasen des oben dargestellten Prozesses für die Auswahl und Einführung von Cloud Diensten. Ein TSF beinhaltet die folgenden drei Komponenten:

- Ermittlung der funktionalen Anforderungen: Die Ermittlung der funktionalen Anforderungen basiert auf der Analyse der Anbieter-Webseite der bisher vom Handwerker eingesetzten Software. Auf dieser Seite sind die Funktionen und Schnittstellen dieser Software i.d.R. aufgelistet und beschrieben. Zur Identifikation der von der bisher genutzten Software angebotenen Funktionen crawlt der TSF die angegebene Webseite und alle darauf verlinkten Seiten der Domäne und gleicht die darauf vorkommenden Wörter mit einer Funktionsontologie ab (semantische Funktionsextraktion).

- Ermittlung der nichtfunktionalen Anforderungen: Auf der Oberfläche werden bestimmte Angaben vom Handwerker (z.B. zu seinem Risikoprofil oder dem subjektiven Wert seiner Daten) erfragt. Anhand dieser Angaben und auf der Grundlage einer Vorgehensweise zur individuellen Ermittlung von (nichtfunktionalen) Anforderungen werden dann diese nichtfunktionalen Anforderungen abgeleitet.

- Suche im Service-Repository: Die funktionalen und nichtfunktionalen Anforderungen bilden zusammen ein umfassendes Suchprofil für die bedarfsgerechte Service-Auswahl. Mittels dieses Suchprofils wird im dritten Schritt ein Abgleich mit allen Diensten durchgeführt, die im Repository des TSF hinterlegt sind. Werden geeignete Dienste gefunden, dann werden diese dem Nutzer auf der Oberfläche präsentiert. Jeder Service in diesem Suchergebnis ist mit einem entsprechenden Link zum Marktplatz auf der CLOUDwerker-Plattform versehen, unter dem der Nutzer den Service bzw. das Service-Bündel buchen kann.

Der Übergang von der zweiten zur dritten Phase des Auswahl- und Einführungsprozesses ist der Zeitpunkt, an dem ein Handwerker vom TSF an die CLOUDwerker-Plattform übergeben wird. Das Buchen, Konfigurieren und die Nutzung des Dienstes findet innerhalb der Plattform statt und basiert auf den entsprechenden Komponenten der Plattform, wie dem Marktplatz, Single-Sign-On und den einzelnen Diensten/Service-Bündeln.

3.3 Wie wird eine Hersteller-Plattform zu einer Offenen Service Plattform?

Möchte ein Hersteller seine Plattform zu einer offenen Service-Plattform umbauen, müssen die Kriterien für Offenheit unter 3.1.1 in der Umsetzung beachtet und ggf. die für den Datenaustausch mit anderen Diensten erforderlichen Schnittstellen implementiert werden. Des Weiteren ist die Erstellung eines Rahmenvertrags notwendig, um die juristischen Aspekte (vgl. 2.6) abzudecken und die Liefer-/Leistungsbeziehung mit anderen Diensteanbietern zu definieren.

4 Integration der Dienste

Ein wichtiges Kriterium für den Erfolg einer Dienste-Plattform ist die Anzahl und der Umfang der angebotenen Dienste. Im Folgenden wird aus Sicht eines Service Providers dargestellt, welche Punkte bei einer Plattform-Integration berücksichtigt werden müssen.

4.1 Wie kann ein Service Provider seine Dienste in die Plattform integrieren?

Als Anbieter eines speziellen Dienstes sollte man zunächst für sich selbst klären, was genau das Ziel bzw. der gewünschte Mehrwert einer Integration des eigenen Angebots in eine Dienste-Plattform ist. Häufig ist dies eine Kombination aus folgenden Aspekten:

- Profitieren von der Präsenz in einer sehr bekannten Serviceplattform zur Erhöhung der eigenen Sichtbarkeit
- Profitieren von gemeinsame Marketingkampagnen / Kundenansprachen in der Plattform
- Verringerung / Vermeidung von Kosten in der Leistungserstellung, z.B. durch Übergabe des Fakturierungsprozesses, des First Level Supports oder sogar des Service Betriebs an den Plattformbetreiber
- Verbesserung des Wertangebots der eigenen Lösung durch Partnering / Bündelung mit anderen Dienstangeboten der Plattform

Sind die eigenen Zielsetzungen klar, so gilt es im nächsten Schritt Probleme und Herausforderungen einer Integration mit der Serviceplattform zu identifizieren und zu bewerten. Die nachfolgende Checkliste fasst die Erkenntnisse des CLOUDwerker Projekts zu den häufigsten Integrationsproblemen, deren Ursachen, sowie möglichen Lösungsansätzen zusammen.

4.1.1 Welche Herausforderungen müssen in Bezug auf die Integration von Diensten überwunden werden?

(i) **Technische Standardschnittstellen für die auf der Plattform angebotenen „Higher Level Services“ (z.B. Fakturierung, CRM) fehlen** bzw. sind aus Konkurrenzabwägungen der einzelnen Anbieter bewusst nicht gewünscht. Für Lower Level Services (z.B. S3 File Storage, Mailversand, Virtual Machine Management, Identity Management, Authentifizierung, Autorisierung) haben sich in den letzten Jahren sehr wohl de-facto Standards etabliert, allerdings sind diese Dienste meist nicht direkt nutzbringend für die Zielgruppe der Handwerker. Es bleibt abzuwarten, ob sich in den nächsten Jahren, auch für Higher-Level-Services Standardschnittstellen bilden. Erste Tendenzen sind erkennbar, z.B. im Bereich der Fakturierung mit dem ZUGFeRD Standard.

Ist das Ziel des Dienstanbieters, seinen Service mit anderen auf der Plattform angebotenen Diensten zu integrieren, um so Nutzenpotentiale für Kunden zu realisieren, so kann das

Fehlen standardisierter Schnittstellen zu anderen Diensten der Plattform ein großes Hemmnis sein. Im Laufe des CLOUDwerker Projekts hat sich gezeigt, dass bereits der Aufwand für die Integration weniger Dienste (z.B. Lexware lexoffice und CAS PIA) aufgrund fehlender Standardschnittstellen sehr hoch ist. Ein Serviceanbieter muss hier also sehr genau evaluieren, wie wertschöpfend (und damit monetarisierbar) eine derartige Integration für Kunden tatsächlich sein kann.

(ii) **Standardisierte AGB, Datenschutzbestimmungen, Kooperationsvereinbarungen, Sicherheitsrichtlinien etc. existieren häufig nicht**. Um den eigenen Dienst in eine Plattform einzubinden, müssen daher häufig zunächst rechtlichen und geschäftlichen Rahmenbedingungen manuell aufeinander abgestimmt werden. Gleiches gilt für die Datenschutzbestimmungen, bei denen vielleicht sogar technische Veränderungen vorgenommen werden müssen (z.B. Betrieb innerhalb eines bestimmten Landes) bevor diesbezügliche Anforderungen des Plattformbetreibers erfüllt werden können.

(iii) **Rahmenbedingungen, Regeln für die Kollaboration unterschiedlichen Anbieter von Diensten im Rahmen von Dienstebündeln müssen festgelegt werden.** Dazu muss beispielsweise festgelegt werden, wer genau einen Kunden ansprechen, ihm Angebote unterbreiten, ihm die erbrachten Dienstleistungen in Rechnung stellen darf und wer für Vertragsverletzungen, Ausfälle etc. haftet. Auch der Umgang mit technischer Weiterentwicklung einzelner Teildienste und wie diese Änderungen dann in komponierte Dienstbündel eingehen sollten spezifiziert werden: Steigt der Preis für das Gesamtbündel? Wer erhält welchen Anteil der Preissteigerung? Wer trägt Kosten für neuerlichen Integrationsaufwand? Müssen neue Security-Audits etc. für das gesamte Dienstbündel durchgeführt werden? Wenn ja, wer macht das?

(iv) **Unterschiedliche Einzeldienste haben sehr unterschiedliche UI Konzepte.** Nachträglich bzw. automatisch komponierte Dienste werden mit Blick auf User Experience (UX) also niemals wie „aus einem Guss“ erscheinen, wenn sie nicht von vorneherein daraufhin angelegt wurden. Gutes UX Design ist jedoch in der Welt der Online Dienste ein entscheidender Faktor für Akzeptanz und Nutzerzufriedenheit.

(v) **Standard-Onboarding-Prozess für Cloud Plattformen / Marktplätze fehlen häufig.** Jede Cloud- Plattform hat ihre eigenen Auditing / Sign-Up / Onboarding-Prozesse (z.B. Telekom Business Market Place vs. Cloudwerker Plattform vs. 1&1 Marktplatz). Keine dieser Plattformen hat jedoch die Marktmacht, einen „De-Facto“ Standard zu setzen. So bleibt für Dienstanbieter nur die aufwändige, individuelle Einbindung seines Dienstes in unterschiedlichen Marktplätzen nach vielen verschiedenen Regeln und Vorgehensweisen. Gebündelt mit nur geringem Marktanteil, der einzelnen Plattformen, ist der Aufwand für die Einbindung im Vergleich zum erwarteten Nutzen für den Dienstanbieter relativ hoch.

4.1.2 Welche Lösungen bzw. Lösungswege werden bereits angeboten?

Mit all diesen Problemen sollten sich Service Provider und Plattformbetreiber beschäftigen und gemeinsam Lösungen erarbeiten. Stand heute ist dem CLOUDwerker Konsortium kein Anbieter bekannt, der eine vertrauenswürdige, vollautomatische Integration und Komposition beliebiger Dienste zu Produktbündeln „aus einem Guss“ anbietet. Dennoch gibt es sichtbare Entwicklungen in diese Richtung.

Auf der einen Seite des Spektrums existieren erste Anbieter von Kommunikationshubs, die über sehr einfache Datenschnittstellen einen ereignisgetrieben Nachrichtenaustausch zwischen

unterschiedlichen Diensten ermöglichen. Beispiele hierfür sind „zapier“ oder „IFTTT“. Auf der Plattform angemeldete Nutzer können dort Regeln der Form „Wenn In Service 1 Ereignis x passiert, führe Aktion y in Service 2 aus“ definieren. So können unterschiedliche Dienste auf einfache Weise zu einem Servicebündel verbunden werden. Die angebotenen Dienste sind dabei weiter völlig unabhängig voneinander, d.h. Abrechnung, Support, Geschäftsbedingungen, Datenschutz etc. sind für jeden Service separat. Zudem ist die Abbildung komplexerer Prozesse bislang nicht möglich.

Auf der anderen Seite des Spektrums stehen vollständige Marktplätze mit einheitlichem Billing, einheitlichen AGBs und einheitlichen Security Standards / Audits. Hierzu zählt z.B. der Telekom Business Marketplace. Bei diesen Ansätzen bekommt ein Kunde tatsächlich alle Dienste aus einer Hand. Im Falle des Telekom Business Marktplace ist sogar der First Level Support vereinheitlicht. Allerdings sind hier die einzelnen Plattformdienste nicht miteinander verbunden, sondern lediglich über eine zentrale Instanz (Telekom) buch- und abrechenbar.

Betrachtet man die eingangs beschriebenen Herausforderungen, die heutigen Lösungsvorschläge vorhandener Anbieter sowie die Erkenntnisse des CLOUDwerker Projekts, so lautet die Empfehlung für potentielle Betreiber einer CLOUDwerker Plattform: „Serviceintegration auf der eigenen Plattform fördern durch Transaktionskostenreduktion“. D.h. das Ziel eines Plattformbetreibers sollte es sein, eine Serviceplattform anzubieten, auf der sowohl das Onboarding neuer Diensteanbieter, als auch die manuelle Komposition von Einzeldiensten der Serviceplattform zu Servicebündeln schnell, einfach und damit kostengünstig macht. In dem Moment, in dem die Transaktionskosten gering sind, ist es (i) einfacher neue Diensteanbieter für die Plattform zu gewinnen und (ii) attraktiver für ein Unternehmen, das eine Marktchance erkennt für, die ein Bündelprodukt aus Einzeldiensten der Plattform eine geeignete Antwort wäre, eben dieses Bündel manuell zu komponieren und wiederum auf der Plattform anzubieten.

4.1.3 Was macht man mit bestehenden (Stamm-)Daten und Plattformdaten

Neben den oben beschriebenen organisatorischen Herausforderungen gilt es bei Integration bestehender Dienste oder Anwendungen in die Plattform eine Reihe konkreter technischer Probleme zu lösen. Wenn ein Handwerker einen Dienst schon über Jahre hinweg genutzt hat, gilt es, neben der eigentlichen Migration des Dienstes auch einen Migrationspfad für die wichtigsten Daten anzubieten.

Sollte es notwendig sein, bestehende Stammdaten in die Plattform zu überführen, muss die Frage der Datenkonsolidierung geklärt werden.

Die mit Abstand am häufigsten zu konsolidierenden Daten sind die Kundendaten. Hierzu bieten sich prinzipiell zwei Strategien an:

- Zunächst Zusammenführen der Kundendaten, anschließend Dublettenauflösung
- Zunächst Ermittlung des Deltas zwischen den beiden Kundenverzeichnissen, anschließend Durchführung der notwendigen Änderungen

Bei beiden Ansätzen und insbesondere bei großen Datenmengen wird es notwendig sein, auf leistungsfähige externe Tools zurückzugreifen. Es gibt spezialisierte Software, die große Datenmengen anhand konfigurierbarer Kriterien auf das Vorhandensein von Dubletten untersuchen kann. Die Einbindung dieser Software und insbesondere die anschließende Auflösung der Dubletten (inklusive ggf. zugehöriger Daten) sind jedoch meist individuell zu lösen.

Es ist auch möglich, ein initiales Mapping der beiden abzugleichenden Datenmengen herzustellen (automatisch, halbautomatisch oder manuell), um anschließend – gewöhnlich auf programmatischem Wege – die Konsolidierung der Daten durchzuführen.

Auch wenn eine regelmäßige Synchronisation eingerichtet werden soll und auf beiden zu synchronisierenden Seiten schon Daten vorhanden sind, muss ein solch initiales Mapping der Datensätze durchgeführt werden.

4.1.4 Wie erfolgt eine technische Integration eines Dienstes in die CWP

Um die Dienste erfolgreich in die Plattform zu integrieren, muss die technische Beschaffenheit und Architektur, wie sie im Gliederungspunkt 3 beschrieben wird, berücksichtigt werden. Insbesondere muss der Dienst um plattformspezifische Elemente erweitert werden, um so die Interoperabilität mit Plattformdiensten zu gewährleisten (siehe obligatorische Zentrale Dienste, Tabelle 1). Im folgenden Abschnitt soll die technische Integration des Dienstes auf verschiedenen Ebenen beschrieben werden. Eingegangen wird auf Backend Integration, Middleware und Frontend Integration.

Backend Integration

Backend Integration bedeutet in diesem Zusammenhang die Ankopplung an Plattformbasisdienste wie z.B. Registry, Authentifizierung, Administrationsfunktionen, Datenbankzugriff usw.

In erster Linie erfolgt im Backend die Orchestrierung. Zudem werden Einstellungen von Sicherheit, Rollen- und Nutzerprofilen und Einstellungen von Servicekomponenten oder allgemeiner Attribute der Dienste wie z.B. Spracheinstellungen übernommen.

Backend Integration lässt sich aber auch auf den Aufruf und die Nutzung anderer Dienste beziehen. Das klassische Beispiel ist die prozessorientierte, sequentielle oder rekursive Verarbeitung von Aufgaben. Hier bekommt der Endnutzer von den im Hintergrund ablaufenden Serviceaufrufen und Serviceantworten im günstigsten Fall nichts mit, sondern es wird lediglich ein Ergebnis an den Frontendservice geliefert. Im ungünstigeren Fall stoppen die im Backend integrierten Dienste, weil zusätzliche Informationen benötigt werden und eine zusätzliche Eingabe des Endnutzers verlangt wird.

Um den vollen Funktionsumfang der Plattform nutzen zu können, müssen zu integrierende Dienste entsprechend der technischen Spezifikation (siehe 3.1.2) über Schnittstellen mit den Plattformbasisdiensten (siehe 3.1.2) verbunden werden.

CLOUDwerker Middleware

Die Middleware besteht aus Diensten, die die Konfiguration der Services auf der Plattform ermöglichen, also z.B. die Aufnahme oder die Bündelung von Diensten auf der Plattform.

Der Use Case des Anwenders entscheidet nicht, wo ein Dienst angesiedelt ist, sondern die Funktion des Dienstes. So kann z.B. ein Dienst auf der Plattform über ein Frontend administriert werden; die Anwendungslogik zur Administration ist in der Middleware implementiert und im Backend wird persistiert.

Frontend Integration

Im Zuge der Frontend Integration soll vor allem auf das für den Nutzer sichtbare Zusammenspiel der Dienste eingegangen werden. Trotz verschiedener Dienste und damit unterschiedlichen Look & Feels sollte dem Nutzer nach Möglichkeit eine Oberfläche zur zentralen Verwaltung und Steuerung der Dienste zur Verfügung gestellt werden. Im Rahmen von CLOUDwerker wurde dafür ein Prototyp eines Marktplatzes geschaffen, der die Dienste in einer Übersicht mit den dazugehörigen Funktionalitäten anzeigt.

Ein einheitliches Frontend über mehre Dienste bzw. Anbieter hinweg (Dienstebündel) stellt jedoch eine große Herausforderung dar, sowohl für techn. Schnittstellen, User Experience als auch Design. Auch wenn die Plattform ein unterstützendes Framework anbietet, sind mit nicht unerheblichen Aufwänden für die Anpassung bereits vorhandener Dienste zu rechnen. Um die Investitionshemschwelle gering zu halten, ist dies keine obligatorische Anforderung für Dienste. Gleichwohl ist damit zu rechnen, dass erfolgreiche Dienstebündel-Anbieter diesen Ansatz weiter verfolgen.

4.2 Wie können on-premise Serviceapplikationen mit der Plattform verknüpft werden?

In manchem Fällen möchte man eine bestehende On-Premise-Lösung um eine Schnittstelle zu Cloudservices erweitern, um beispielsweise bestimmte Daten mit den Cloudservices zu teilen oder bestimmte Funktionen überall verfügbar zu machen.

Am Beispiel „Lexware eCRM“ soll dargestellt werden, wie eine solche Erweiterung für Lexware-Produkte realisiert wurde.

Lexware hat verschiedene ERP-Produkte im Angebot, die um eine CRM-Funktionalität erweitert wurden. Die CRM-Funktionalität wird über eine Cloud-Anwendung „eCRM“ zur Verfügung gestellt. Es handelt sich dabei um eine angepasst Version der CRM-Software „CAS PIA“.

Die Lexware-ERP-Produkte können dabei folgende Daten mit eCRM synchronisieren:

- Kunden- bzw. Adressdaten
- Dokumente bzw. Belege
- Projekte

Dabei kann prinzipiell in beide Richtungen synchronisiert werden. Allerdings sind die Berechtigungen zur Bearbeitung der Daten in den beiden Anwendungen unterschiedlich. So z.B. können Belege zwar in CAS PIA eingesehen, nicht aber bearbeitet werden, was nur in Lexware möglich ist.

Der Abgleich der Daten zwischen der On-Premise-ERP-Software und eCRM erfolgt dabei manuell angestoßen aus dem ERP-Produkt heraus. Technisch gesprochen wird von der ERP-Software eine WebService-Schnittstelle von eCRM verwendet, um Daten von eCRM abzurufen bzw. dort zu speichern. Es wird also der gleiche Ansatz verfolgt wie er auch bei der CWP realisiert wurde: Die Plattform (bzw. eCRM) bietet eine standardisierte Schnittstelle, über die Daten abgerufen, erzeugt und verändert werden können. Alle ERP-Produkte verwenden diese Schnittstelle. Somit greifen alle ERP-Produkte auf die gleiche Datenbasis zu.

Das Login in eCRM erfolgt ebenfalls aus der ERP-Software heraus. Über einen Single-Sign-On-Mechanismus wird der Benutzer dabei automatisch an eCRM angemeldet.

Nachdem die Kundendaten von der ERP-Software nach eCRM transferiert wurden, werden in eCRM gezielt CRM-Funktionen wie Terminvereinbarung, Kundenakten oder Kampagnendurchführung verwendet.

4.2.1 Dienste Migration

Die meisten Handwerker arbeiten heute mit einer Vielzahl von Anwendungen. Meistens handelt es sich dabei um On-Premise-Anwendungen. CLOUDwerker ist eine Cloud-basierte Plattform, d.h. eine Reihe von Anwendungen, die im Internet nach weitgehend gleichen technischen Regeln laufen und über eine gemeinsame Plattform erreichbar sind.

Für den Handwerker als Anwender bedeutet das, dass er mit einer Reihe an Umstellungen umgehen muss. Falls seine bestehende On-Premise-Anwendung auf die Plattform migriert wird, stehen die Chancen gut, dass er sich weiterhin in seiner vertrauten Arbeitsumgebung bewegen kann. Vermutlich werden allerdings zumindest ein paar weitere Dienste hinzukommen, wie er zukünftig verwenden möchte, die eine entsprechende Einarbeitung erfordern.

Möglicherweise wird die zukünftige Arbeitsumgebung – ggf. nach einer entsprechenden Datenmigration – für den Handwerker jedoch eine gänzlich neue sein.

Neben den technischen Herausforderungen sind deshalb gleichermaßen eine Reihe weiterer Herausforderungen zu meistern, um die Migration erfolgreich gestalten zu können.

Im Dokument *„AP 3.3, Anwendungsmigration & Komposition, Kapitel 2: Nicht-technische Aspekte der Anwendungs-Migration*“ ist der Prozess der Softwareeinführung in vier verschiedenen Dimensionen ausgearbeitet. Es wird unterschieden in fachliche, psychologische, organisatorische und technische Dimensionen.

Am Beispiel einer Handwerkersoftware werden die einzelnen Dimensionen detailliert aufgeschlüsselt und beschrieben. Aus diesem Beispiel lassen sich generische Ableitungen für mögliche weitere Softwareeinführungsprozesse machen.

Weitere Details können im Dokument *AP 3.3 Anwendungsmigration & Komposition* nachgelesen werden.

4.3 Testkonzept

Eine wichtige Charakteristik der Offenen Plattform ist, dass das System durch Anwendungsdienste dynamisch erweitert werden kann. Aus diesem Grund sind nicht nur Tests notwendig, welche die einzelnen Dienste auf korrekte Funktionalität und Konformität überprüfen, es werden auch Tests benötigt, mit denen die Verlässlichkeit des Gesamtsystems überprüft werden kann. Weiterhin muss auf eine ausreichende Performanz der Anwenderdienste unter realistischer Nutzungslast geachtet werden, die sich erst aus dem Zusammenspiel mit den Basisdiensten und aus den zur Verfügung stehenden Ressourcen der Cloud ergibt.

Eine Herausforderung besteht darin, Dienste innerhalb einer dienstbasierten Architektur auf korrekte und protokollkonforme *Funktionalität* sowie einen geforderten Grad an *Verlässlichkeit* zu testen. Dadurch, dass die Dienste in einer Cloud-Umgebung ausgeführt werden, ergibt sich zudem eine dritte Herausforderung, das Feststellen der zu erwartenden *Performanz* der Gesamtanwendung im Betrieb und ihre Skalierbarkeit bei steigenden Nutzerzahlen. Nachfolgend werden Ansätze vorgeschlagen,

mit denen Dienste hinsichtlich der Qualitätsattribute Funktionalität, Verlässlichkeit und Performanz bzw. Skalierbarkeit untersucht werden können.

(i) "Hält sich eine Komponente an die vereinbarten Standardprotokolle und -schnittstellen?" Bevor ein Dienst im Marktplatz angeboten werden kann, gilt es sicherzustellen, dass er sich an die erforderlichen Richtlinien der Plattform hält und die vereinbarte *Funktionalität* in der erwarteten Weise an der Schnittstelle bereitstellt. Hierzu kann die Komponente einer Serie von Unit-Tests unterzogen werden, welche die Komponente auf gültige Interaktionsmuster und die spezifizierte Funktionalität prüft. Je nach Anwendungsfall können an dieser Stelle Blackbox-, Graybox- und Whitebox-Techniken eingesetzt werden.

(ii) "Wie wirkt sich eine angebotene Komponente auf die Verlässlichkeit des Gesamtsystems aus?" Fehler, die bei der Kommunikation von Diensten untereinander auftreten können, sind auf Grund der hohen Zahl möglicher Interaktionen nur schwer systematisch testbar. Zwar können Integrationstestfälle eingesetzt werden, diese repräsentieren jedoch bei Weitem nicht die alltägliche Nutzung, womit keine zuverlässige Aussage über die *Verlässlichkeit* des Gesamtsystems gemacht werden kann. An dieser Stelle kann das sogenannte *statistische Whitebox-Testen* verwendet werden, um eine höhere Testabdeckung zu erreichen. Das statistische Whitebox-Testen kombiniert das bereits bekannte statistische nutzungsbasierte Testen mit der automatischen Erzeugung von Testmustern auf der Basis der symbolischen Ausführung (Symbolic Execution). Ziel des Ansatzes ist es, eine möglichst hohe Abdeckung solcher Codepfade zu erreichen, welche in den geplanten Nutzungsszenarien ausgeführt werden. Die für den Ansatz erforderlichen Nutzungsszenarien (Usage Models) lassen sich im Palladiomodell spezifizieren. Dieser neuartige Ansatz wurde im Rahmen des CLOUDwerker-Projekts erarbeitet [Omri2013]. Ein wichtiges Einsatzgebiet bei CLOUDwerker ist die ausgiebige Prüfung der Basisdienste in Kombination mit einem Bündel von Anwenderdiensten, um Aussagen über die Verlässlichkeit eines angebotenen Bündels machen zu können.

(iii) "Welchen Einfluss hat der Dienst auf die Performanz und Skalierbarkeit des Gesamtsystems?" Bereits ein einzelner Dienst kann sich negativ auf die Gesamtlast und damit die Betriebskosten, bzw. aus Nutzersicht – je nach Konfiguration der Cloud – auf die Latenz des Systems auswirken. Um sicherzustellen, dass ein Dienst in geplanten Szenarien ausreichend performant ist und die Skalierbarkeit innerhalb der Cloud gewährleistet wird, können die für das statistische Whitebox-Testen bereits spezifizierten Nutzungsszenarien wiederverwendet werden, um daraus Lastpläne abzuleiten. Ein Ansatz, der sich hierfür besonders anbietet, ist *CloudScale* [Brataas2013], da er, wie schon das statistische Whitebox-Testen, ebenfalls auf Nutzungsmodelle des Palladio-Architekturmodells zurückgreift. CloudScale zieht den Kontroll- und Datenfluss der Anwendung sowie die Eigenschaften der Cloud-Umgebung in seine Simulation mit ein, um potentielle Performanz- und Skalierbarkeitsprobleme frühzeitig vor dem geplanten Betrieb zu erkennen. Somit können rechtzeitig Entwurfsfehler erkannt werden, die sich in erhöhten Kosten (verursacht durch ein *Overprovisioning*) oder erhöhten Reaktionszeiten (verursacht durch ein *Underprovisioning*) bemerkbar machen.

5 Zusammenfassung

Der Einsatz von CLOUD-Technologien ist bei kleinen Handwerksunternehmen bislang wenig ausgeprägt. CLOUD-Technologien können jedoch dabei unterstützen, Bürotätigkeiten und Aufträge effizient abzuwickeln. Daher wurde im Rahmen des CLOUDwerker-Projekts eine vertrauenswürdige, offene Service-Plattform unter Verwendung und Erweiterung von Cloud-Technologien konzipiert und prototypisch umgesetzt, um Handwerker das Zusammenstellen und komfortable Buchen benötigter Dienste-/bündel zu ermöglichen und sie so bei ihrer Arbeit zu unterstützen.

Der Service-Provider Leitfaden hat die verschiedenen technischen und nicht-technischen Aspekte systematisch durchleuchtet, die bei der Umsetzung und Betrieb einer Service-Plattformen bzw. der Bereitstellung von Dienstbündeln zu beachten sind. Das Sicherstellen der Vertrauenswürdigkeit sowie die sorgfältige Auswahl der Dienste sind dabei eine wichtige Voraussetzung für den Betrieb einer Plattform, weshalb auch auf diesbezüglich relevante Kriterien eingegangen wurde. Außerdem wurden die Möglichkeiten beschrieben, wie man On-Premise-Applikationen mit der Plattform verknüpfen kann.

Softwaredienstleistern und Plattformanbietern sollte es mit Hilfe des Service-Leitfadens nun möglich sein, eine eigene Plattform aufzubauen oder Dienste in eine vorhandene zu integrieren und erfolgreich zu betreiben.

Glossar

CRM	Customer Relationship Management, Kundenverwaltung
CWP	CLOUDwerker Plattform
ERP	Enterprise Ressource Planning, Warenwirtschaftssystem
HIP	Host Identity Protocol
ISO	Internationale Standardisierungsorganisation
KIT	Karlsruhe Institut für Technologie
SaaS	Software as a Service, Software als Dienst, Softwaredienst
PaaS	Platform as a Service, Cloud Plattform als Dienst, Plattform
IaaS	Infrastructure as a Service, virtualisierte Server und Speicher

Literaturverzeichnis

[Christm2014] Christmann, Constantin; Horch, Andrea; Kett, Holger; Falkner, Jürgen; Weisbecker, Anette: Auswahl vertrauenswürdiger Cloud Services im Handwerk - Ein Leitfaden für Handwerker und ihre Berater. Stuttgart: Fraunhofer Verlag, 2014.

[Omri2013] Fouad ben Nasr Omri, Ralf Reussner. Towards Reliability Estimation of Large Systems-of-Systems with The Palladio Component Model. Workshop "Wissenschaftliche Ergebnisse der Trusted Cloud Initiative", Karlsruhe, Germany. 2013.

[Brataas2013] Gunnar Brataas, Erlend Stav, Sebastian Lehrig, Steffen Becker, Goran Kopčak, and Darko Huljenic. CloudScale: scalability management for cloud systems. In Proceedings of the 4th ACM/SPEC International Conference on Performance Engineering (ICPE '13), Seetharami Seelam (Ed.). ACM, New York, NY, USA, 335-338. 2013.

Anhang

Rechtliche Rahmenbedingungen für Anbieter von Cloud-Diensten

Cloud-Dienste (auch „Software as a Service“ genannt) erfreuen sich immer größerer Beliebtheit. Aufgrund der aktuellen Entwicklungen und immer häufigeren Meldungen über Datenpannen achten allerdings auch immer mehr private und gewerbliche Kunden bei der Auswahl des Anbieters der jeweiligen Cloud-Dienste auf eine datenschutzkonforme und sichere Speicherung und Verarbeitung ihrer Daten, beziehungsweise eine interessengerechte Vertragsgestaltung.

Für Anbieter von Cloud-Diensten haben sich insoweit spezifische rechtliche Anforderungen herausgebildet, die zwischenzeitlich als Mindeststandard für entsprechende Angebote in Deutschland angesehen werden können.

Nachfolgend sollen deshalb die wesentlichen rechtlichen Implikationen zusammengefasst werden, die von Anbietern entsprechender Cloud-Dienste beachtet und im Rahmen ihrer Vertragsgestaltung, aber auch bei der technischen Konfiguration der Dienste umgesetzt werden sollten.

I. Datenschutz

Die Zulässigkeit von Cloud-Diensten ist vor allem von der Erfüllung datenschutzrechtlicher Grundsätze abhängig. Die rechtlichen Rahmenbedingungen hierzu finden sich in den §§ 3, 9 und 11 des Bundesdatenschutzgesetzes (BDSG).

1. Welche Daten sind betroffen?

   Datenschutzrechtliche Grundsätze greifen nur ein, wenn auch personenbezogene Daten in der Cloud verarbeitet werden sollen. Personenbezogen sind Daten, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, also vor allem Kunden- oder Mitarbeiterdaten. Entsprechende Daten dürfen nur in der Cloud verarbeitet und damit an den jeweiligen Cloud-Anbieter „weitergegeben“ werden, wenn eine entsprechende gesetzliche Legitimation vorliegt.

   Sollen also in der Cloud des jeweiligen Anbieters Daten über Kunden oder Arbeitnehmer ohne ausdrückliche Einwilligung gespeichert werden, unterliegt dies strengen Datenschutzregeln. Bei der Übermittlung, Verarbeitung und Speicherung solcher personenbezogener Daten ist vom Anbieter sicherzustellen, dass der Nutzer „Herr der Daten“, also Verantwortlicher, bleibt.

   Aus Sicht des Datenschutzes kommt es dabei entscheidend auch auf den Ort der jeweiligen Datenspeicherung und -verarbeitung an. Bei Cloud-Services ist dies aber gerade nicht so leicht zu beherrschen, weil der Nutzer eben gerade keinen unmittelbaren Einfluss darauf hat, wo genau die Daten am Ende gespeichert werden.

   Für die Einhaltung der oben genannten datenschutzrechtlichen Anforderungen ist seitens des Anbieters deshalb darauf zu achten, dass die Daten nur in Ländern gespeichert werden, die ein angemessenes Datenschutzniveau gewährleisten. Vor diesem Hintergrund ist es sinnvoll, die

Daten ausschließlich auf solchen Servern zu speichern und zu verarbeiten, die innerhalb des Europäischen Wirtschaftsraumes (EWR) liegen.

Sollte der Anbieter auch Server außerhalb Europas einsetzen wollen, sollte zumindest über eine entsprechende vertragliche Gestaltung das Erreichen eines entsprechenden Datenschutzniveaus sichergestellt werden (z. B. über die Aufnahme der EU-Standardvertragsklauseln oder entsprechende Binding Corporate Rules (= verbindliche Unternehmensrichtlinien)).

Festzuhalten bleibt, dass Anbieter von Cloud-Diensten, deren Server ausschließlich im Europäischen Wirtschaftsraum liegen, entsprechende datenschutzrechtliche Privilegierungen und damit ein besonderes Vertrauen genießen.

2. Angebot einer Auftragsdatenverarbeitungsvereinbarung

Nach dem BDSG ist es seitens des Anbieters regelmäßig erforderlich, mit dem Nutzer eine sogenannte Auftragsdatenverarbeitungsvereinbarung zu schließen.

Der Cloud-Anbieter gilt damit rechtlich als verlängerter Arm des die Cloud nutzenden Kunden. Der Mindestinhalt einer solchen Vereinbarung ist in § 11 BDSG geregelt. Hierzu gehören etwa die Festlegungen hinsichtlich Art, Ort und Umfang der Datenverarbeitung. Anbieter von Cloud-Diensten sollten insoweit im Vorfeld entsprechende Auftragsdatenverarbeitungsvereinbarungen vorbereiten, die dann als mit dem Nutzer zu schließende Muster übersandt werden. Grundsätzlich ist diese Möglichkeit der Auftragsdatenverarbeitung aber nur mit einem Cloud-Anbieter innerhalb des Europäischen Wirtschaftsraums möglich. Auch insoweit sind Anbieter mit Sitz in Europa also privilegiert.

Als wichtiges Kriterium für die Rechtskonformität und die Vertrauenswürdigkeit eines Cloud-Anbieters ist deshalb von besonderer Bedeutung, dass dieser dem Kunden den Abschluss einer entsprechenden Auftragsdatenverarbeitungsvereinbarung mit den genannten Inhalten anbietet.

3. Zertifizierung eines Anbieters

Unternehmen die Cloud-Dienste einsetzen müssen nach dem Datenschutzrecht ihre Anbieter sorgfältig auswählen und regelmäßig überprüfen. Diese Auswahl- und Prüfpflicht umfasst auch Regelungen zu technischen und organisatorischen Sicherheitsmaßnahmen.

Da den Kunden bisweilen das notwendige Wissen fehlt, um die Erfüllung dieser Vorgaben zu beurteilen, erscheint es als ein besonderes Kriterium für die Datensicherheit und Vertrauenswürdigkeit eines Anbieters, wenn er die Erfüllung der entsprechenden Vorgaben selbst gewährleistet. Der Anbieter kann die Prüfpflicht der Kunden dadurch ersetzen, wenn er ein eigenes Datenschutzkonzept vorweisen kann und/oder von einer unabhängigen Stelle zertifiziert wurde.

Anbieter von Cloud-Diensten ist insoweit zu empfehlen, entsprechende Zertifikate zu erwerben (z. B. Trusted Cloud, ISO 27001 u. a.), diese aktuell zu halten, regelmäßig zu erneuern und den

potenziellen Kunden als besonderen Beleg der Datensicherheit und dem Vorliegen eines Datenschutzkonzeptes zur Verfügung zu stellen.

4. Verschlüsselung von Daten

§ 9 BDSG schreibt vor, dass der Schutz personenbezogener Daten durch entsprechende technische und organisatorische Maßnahmen zu gewährleisten ist.

Dementsprechend sollte der Anbieter von Cloud-Diensten geeignete Maßnahmen auch auf technischer Ebene sicherstellen. So ist zum Schutz vor einem unberechtigten Zugriff zum Beispiel darauf zu achten, dass die Daten nur verschlüsselt gespeichert und übermittelt werden. Dies schützt nicht zuletzt auch vor dem „Diebstahl" etwaigen Know-How der Kunden und einer widerrechtlichen Weitergabe von Geschäfts- und Betriebsgeheimnissen.

Damit stellt sich eine hinreichende Verschlüsselung der Daten als besonderes Kriterium für die Vertrauenswürdigkeit von Cloud-Diensten dar.

II. Vertragsgestaltung

Bei der Gestaltung der Verträge sollten Anbieter darauf Wert legen, dass diese den konkreten Anforderungen der avisierten Kunden entsprechen. Je nachdem, welcher Branche die potentielle Kunden zuzuordnen sind, sind möglicherweise auch besondere gesetzliche Anforderungen zu erfüllen (z. B. Rechtsanwälte und Steuerberater, Banken o.ä.).

1. Service Level Agreements

Der Zugriff auf die Daten hängt für den Kunden entscheidend von der Verfügbarkeit des Cloud-Dienstes ab. Daher sollte jeder Anbieter spezifische Gewährleistungsregelungen (sog. Service Level Agreements) in seine Verträge aufnehmen, was im Falle eines Systemausfalles als Rechtsfolge vorgesehen ist und ob Verfügbarkeitsgarantieren übernommen werden. Da der Kunde im Falle eines (längerfristigen) Serverausfalls möglicherweise auf unternehmenskritische Informationen nicht zugreifen kann, bis der Fehler durch den Anbieter wieder behoben ist, sind entsprechende Service Level Agreements für diesen von besonderer Bedeutung.

Auch ein Sicherheitskonzept und eine genaue Beschreibung der insoweit getroffenen technischen Vorkehrungen sollte in den Vertrag aufgenommen werden. Hierzu gehören auch entsprechende Angaben zu Pflege- und Fehlerbeseitigungsmaßnahmen, sowie Maßnahmen zur Abwehr von Angriffen und Störungen. Besonders vertrauenswürdig ist der Anbieter, wenn er diese Maßnahmen durch zusätzliche Haftungsübernahmen und/oder Vertragsstrafen absichert.

2. Rechtswahl und Gerichtsstand

Nicht zu vernachlässigen ist auch die Frage, welchem Recht der Vertrag unterliegt. Im besten Fall sollte der Vertrag bei deutschen Nutzern die Anwendbarkeit deutschen Rechts vorsehen, um das

Risiko für den Kunden auszuschließen, einen Rechtsstreit in einem fremden Recht führen zu müssen.

Daneben sollte auch auf den Gerichtsstand, also den Ort einer möglichen rechtlichen Auseinandersetzung, geachtet werden.

3. Kündigung

Der Vertrag des jeweiligen Cloud-Anbieters sollte klare Kündigungsregeln enthalten. Die entsprechenden Klauseln sollten nicht nur festlegen, wie und mit welchen Fristen der Nutzungsvertrag gekündigt werden kann, sondern auch bestimmen, welche Regelungen der Vertrag für den Fall der Kündigung vorsieht. Von besonderer Bedeutung ist hier, ob dem Kunden eine Möglichkeit zum Export seiner Daten eingeräumt wird. Aus Kundensicht wird es zwischenzeitlich auch als wichtiges Kriterium angesehen, wenn ein Umzug zu einem anderen Anbieter gewährleistet werden kann. Im besten Falle, sollte der Anbieter Hilfe beim Umzug leisten.

Um Vertrauen zu schaffen, sollte der Vertrag auch eine ausdrückliche Regelung enthalten, dass der Kunde „Eigentümer“ der Daten bleibt, dass und wie diese im Falle einer Kündigung vollständig herausgegeben werden bzw. im Anschluss beim Anbieter endgültig gelöscht werden.

4. Urheberrecht

Für die Nutzung der Cloud-Dienste ist seitens des Kunden grundsätzlich kein Erwerb von Lizenzen für die Benutzung des Dienstes erforderlich.

In urheberrechtlicher Hinsicht hat jedoch der Anbieter sicherzustellen, dass die von ihm zur Verfügung gestellten Softwareanwendungen für den konkreten Einsatz, nämlich die Bereitstellung im Internet für eine Vielzahl von Kunden, verwendet werden dürfen.

Urheberrechtlich unproblematisch ist dies, wenn und soweit die Software und auch alle entsprechenden Bestandteile von dem jeweiligen Anbieter selbst stammen, dieser also auch gleichzeitig Softwarehersteller ist.

Wenn und soweit der Anbieter auch fremde Softwareanwendungen über die jeweilige Cloud zur Verfügung stellen möchte, hat er sich vom Rechteinhaber entsprechende Nutzungsrechte einräumen zu lassen. Aufgrund der Bereitstellung etwaiger Fremdsoftware über die Cloud zur Nutzung durch entsprechende Kunden, werden in jedem Fall die §§ 19 a, 69 c Nr. 4 UrhG, die die öffentliche Zugänglichmachung von urheberrechtlich geschützten Werken regeln, einschlägig sein.

Wenn der Cloud-Anbieter selbst oder durch beauftragte Dritte Open Source Software (OSS) oder entsprechende Komponenten integrieren bzw. zur Nutzung anbieten will, hat er sicherzustellen, dass die jeweiligen OSS-Lizenzbedingungen eingehalten werden.

Bei der Verwendung von OSS seitens des Cloud-Anbieters ist insoweit eine Untersuchung der Anforderungen wichtig, weil einige der OSS-Lizenzen – gewissermaßen als Ausgleich für die kostenlose Nutzungsrechtseinräumung – einen Vertrieb der unter der Verwendung der OSS-Komponenten entwickelten Software nur unter der Voraussetzung gestatten, dass die Nutzungsrechte am Quellcode dieser Entwicklung in ihrer Gesamtheit ebenfalls jedermann unentgeltlich zu Verfügung gestellt werden (sog. Copyleft Lizenzen). Diese Ansteckung der Gesamtsoftware wird auch als viraler Effekt der Copyleft Lizenzen bezeichnet.

Im Hinblick auf das Urheberrecht ist mithin zusammenzufassen, dass der Anbieter dafür Sorge zu tragen hat, dass ihm vertraglich sämtliche Nutzungsrechte eingeräumt worden sind, die er zur öffentlichen Zugänglichmachung über den jeweiligen Cloud-Dienst gegenüber dem Kunden benötigt.

III. Zusammenfassung

Bei Berücksichtigung der vorgenannten rechtlichen Rahmenbedingungen, die in der nachfolgenden Checkliste auch noch einmal zusammengefasst werden, stehen dem Angebot von Cloud-Diensten auch aus rechtlicher Sicht keine grundsätzlichen Hindernisse entgegen.

Checkliste

	JA	NEIN	UNKLAR
Datenschutz			
Sollen im Rahmen des Cloud-Dienstes auch personenbezogene oder geheimhaltungsbedürftige Daten gespeichert oder verarbeitet werden?			
• Transaktionsdaten			
• Kundendaten			
• Mitarbeiterdaten			
• Geschäftsgeheimnisse			
Stehen die Server des Anbieters innerhalb des Europäischen Wirtschaftsraums (EWR)?			
• Deutschland			
• Europa			
Ist ein hinreichendes Datenschutzniveau sichergestellt, wenn die Server nicht innerhalb des Europäischen Wirtschaftsraumes liegen?			
Werden EU-Standardvertragsklauseln oder Binding Corporate Rules verwendet?			
Kann der Kunde einen Auftragsdatenverarbeitungsvertrag abschließen?			
Enthält der Auftragsdatenverarbeitungsvertrag die notwendigen Regelungen (§ 9 BDSG)?			
Ist die Zutrittskontrolle vom Cloud-Anbieter geregelt?			
Ist die Zugangskontrolle vom Cloud-Anbieter geregelt?			
Ist die Zugriffskontrolle vom Cloud-Anbieter geregelt?			
Ist die Weitergabekontrolle vom Cloud-Anbieter geregelt?			
Ist die Eingabekontrolle vom Cloud-Anbieter geregelt?			
Ist die Auftragskontrolle vom Cloud-Anbieter geregelt?			
Ist die Verfügbarkeitskontrolle vom Cloud-Anbieter geregelt?			
Ist das Prinzip der Zweckbindung vom Cloud-Anbieter geregelt?			
Gibt es ein Datenschutzkonzept?			
Ist der Anbieter zertifiziert und ist das Zertifikat aktuell?			

Werden die Daten bei der Übertragung verschlüsselt?			
Vertragsgestaltung			
Werden die wesentlichen Leistungen angeboten?			
• Alle notwendigen Leistungen sind im Vertrag enthalten			
• Für manche Leistungen muss zusätzlich auf andere Anbieter zurückgegriffen werden			
Sind die Verfügbarkeitsregeln und die Service-Level-Vereinbarungen ausreichend?			
Gibt es sonstige Garantien oder freiwillige Selbstverpflichtungen?			
Gibt es ein Sicherheitskonzept?			
Ist das Sicherheitskonzept durch organisatorische und technische Vorkehrungen abgesichert?			
Welchem Recht unterliegt der Vertrag?			
• Deutschem Recht			
• Europäischem Recht			
• US-Amerikanischem Recht			
• Internationalem Recht (ohne Europa und USA)			
Wo ist der Gerichtsstand des Anbieters?			
• Deutschland			
• Europa			
Bestehen Mindestvertragslaufzeiten die eingehalten werden müssen?			
Gibt es Kündigungsmöglichkeiten innerhalb der Mindestvertragslaufzeiten?			
Kann der Anbieter ohne schwerwiegende Hürden gewechselt werden?			
Gibt es ein einfaches und transparentes Übergabeprozedere?			
Sieht der Vertrag eine Löschung der Daten vor?			
Urheberrecht			
Sind die für den Cloud-Dienst erforderlichen urheberrechtlichen Nutzungsrechte eingeräumt?			
Ist Fremdsoftware im Rahmen des Cloud-Angebotes integriert?			

Ist Open-Source Software (OSS) im Rahmen des Cloud-Angebotes integriert und sind etwaige virale Effekte berücksichtigt?			

CLOUDwerker

Projektpartner