STANDARDS ALS HILFESTELLUNG FÜR CLOUD-COMPUTING | WHITE PAPER

Ihr Experte für die digitale Transformation im Cloud-Ecosystem:

Diese Seite wurde zur besseren Lesbarkeit der Folgeseiten
in der doppelseitigen Darstellung eingefügt.

Inhalt

1. INTENTION DES **WHITE PAPERS**

Aus der Erfahrung ist bekannt, dass Standards Märkte treiben können, fehlende Standards hingegen ausbremsen. Der Siegeszug von VHS, der Audio-CD oder der Video-DVD wäre ohne Standardisierung nicht vorstellbar gewesen. Individueller Autoverkehr ohne Normen für das Benzin wäre ebenso wenig möglich, wie der Einkauf von Elektrogeräten ohne Standards für den Strom aus der Steckdose.

Das vorliegende White Paper widmet sich daher der Frage, welche Bedeutung Standards für Cloud Computing haben und welche dafür wichtig sind. Obwohl das Cloud Ecosystem derzeit nicht den Anspruch hegt, eigene Standards zu verfolgen, soll es dennoch zur Diskussion über sinnvolle Standards im Kontext Cloud anregen. Ein Forum für diese Diskussion bietet der Arbeitskreis (Eco-Cluster) Standards & Integration, zu dem alle Mitglieder des Cloud Ecosystem herzlich eingeladen sind. Es wird daher ein dynamisches Dokument werden: Updates werden dem Diskussionsstand innerhalb und außerhalb des Cloud Ecosystems folgen. Zudem sind Hinweise und aktive Mitarbeit an zukünftigen Versionen ausdrücklich erwünscht!

Neben einer kurzen Einführung über die Vor- und Nachteile von Standards wird ein Überblick über für Cloud Computing wichtige Standardisierungsbereiche gegeben. Ergänzt werden die Standardisierungsbereiche durch aktuelle Einschätzungen über für diese Bereiche bestehende Standards oder bekannte Normungsvorhaben.

Aufgrund des breiten Interesses am Thema und der Breite des Themas „Cloud“ wurden in den letzten Jahren diverse Standardisierungsbemühungen und Leitfäden publiziert, die sich teils an Programmierer, teils an Nutzer wenden. Zudem gibt es eine Vielzahl Standards, die einen Bezug zur Cloud Thematik aufweisen, jedoch nicht explizit dafür entwickelt wurden. Diese Zielrichtungen gegeneinander abzugrenzen mag von akademischem Interesse sein, spielt für die praktische Nutzung jedoch eine eher untergeordnete Rolle: Sollte man einen guten allgemeinen Standard nicht nutzen, nur weil er nicht explizit für die Cloud entwickelt wurde? Wohl kaum!

Einen guten Überblick zur Cloud Standardisierungslandschaft hat das Bundesministerium für Wirtschaft und Technologie herausgegeben, unter dem Titel „Das Normungs- und Standardisierungsumfeld von Cloud Computing“. Es wurde 2012 herausgegeben, womit ein Teil des Dilemmas offensichtlich wird: Drei Jahre sind für Cloud Computing eine lange Zeit, in der die Aktualität schnell droht, verloren zu gehen.

Aufgrund der dynamischen Entwicklung, die Technik, Geschäftsmodelle und gesetzliche Rahmenbedingungen gleichermaßen umfasst, kann das vorliegende White Paper daher nur eine Momentaufnahme sein. In allen Bereichen erfolgen permanent Updates. Deshalb liegt der Schwerpunkt der Darstellung auf den Grundlagen und der Orientierung in Hinblick auf das Angebot und die Nutzung von Clouds.
Es hat nicht den Anspruch auf Vollständigkeit und akademische Darstellung, sondern versucht eher ein praxisnaher Kommentar zur Cloud- „Szene“ zu sein. Details können und sollten in den jeweils aktuellen Fassungen der Standards nachvollzogen werden. Ergänzungen und Anregungen werden vorbehaltlich der fachlichen und redaktionellen Prüfung gerne entgegen genommen. Interessenten an einer Mitarbeit im Arbeitskreis (Eco-Cluster) Standards & Integration bitten wir ebenfalls um Kontaktaufnahme!

Kontakt:
Folker Scholz
fscholz@folkerscholz.de

Dank:
Mein besonderer Dank für fachliche Hinweise und Diskussionen gilt:

Bernhard Cygan, StoneOne AG
Ralf Hülsmann, Deutsche Telekom AG
Andreas Liebing, StoneOne AG
Wolfgang Schmidt, X-Integrate GmbH

2. STANDARDS

Standardisierung dient vor allem der Vereinfachung. Standards bieten Verlässlichkeit zwischen unterschiedlichen Marktteilnehmern. Sie helfen sowohl zwischen Kunden und Anbietern als auch zwischen Anbietern. Vor allem Standards für die Verbindung von Komponenten reduzieren den Aufwand für die Anbieter. Arbeitsteilung und die damit oftmals verbundene Modularisierung von Produkten und Leistungen sind ohne Normen und Standards kaum umsetzbar. Kunden helfen Standards, wenn es darum geht, Leistungen zu beurteilen oder Verträge zu prüfen. Auditoren arbeiten mit Standards. Prüfsiegel sind ohne Standards undenkbar. Egal, ob es sich um die Normung von Schraubgewinden, Steckern, Prüfsiegel oder den Austausch von Daten geht: Standards erhöhen die Effizienz verteilter Leistungs-Erbringung und Inanspruchnahme.

Es sollte allerdings nicht verschwiegen werden, dass Standards zwar auf der einen Seite verlässliche Stabilität erzeugen, jedoch auf der anderen Seite Innovationen einschränken können. Deshalb sind auch Standards regelmäßig auf ihre Angemessenheit hin zu prüfen und entsprechend dem aktuellen Stand der Erkenntnisse ggf. anzupassen. So kann beispielsweise die Erkenntnis von Schädigungen durch eine Chemikalie zu neuen Grenzwerten in Umweltstandards führen. Genauso verändert Cloud Computing die Anpassung von IT-Normen.

Der internationale Zusammenschluss von Normungsinstituten „ISO“ (International Organization for Standardization[1]) hatte beispielsweise Standards für IT-Sicherheit entwickelt. Im Zuge der zunehmenden Nutzung von Clouds wurden jedoch weitere Cloud-spezifische Standards entwickelt, die sowohl die bestehenden ergänzen als auch neue Aspekte aufgreifen.

Erfahrungsgemäß dauern internationale Normungen recht lange. Zuerst muss es eine Initiative geben. Dann werden Teilnehmer eingeladen, die häufig Repräsentanten von nationalen Normungsbehörden, Verbänden und anderen Interessengruppen sind und daher nur einen begrenzten Teil ihrer Ressourcen für ein Standardisierungsvorhaben aufbringen können. Arbeitsgruppen werden gebildet, die Entwürfe produzieren. Die Entwürfe pendeln zwischen den nationalen Komitees und teilnehmenden Verbänden, die ihrerseits die Vorschläge an fachliche oder lokale Sub-Arbeitsgruppen zur Kommentierung weiterreichen. Zwischen den Sitzungen liegen Wochen und Monate, so dass internationale Standard oft Jahre brauchen, bis aus einer Initiative ein veröffentlichter Standard wird.[2] Es ist leicht nachvollziehbar, dass in einem dynamischen Umfeld mithin die Gefahr besteht, dass Standards entweder zum Zeitpunkt der Veröffentlichung nicht mehr ganz aktuell sind oder aber sich auf eher generische Positionen zurückziehen. Zudem fließen in den Normungsprozess Sichtweisen und Interessen mehrerer Dutzend Experten und manchmal auch Lobbyisten ein, die oftmals wirklich jede Nische eines Themas beleuchten. Diesen Umständen geschuldet vermitteln große internationale Standards manchmal bei den Nutzern den Eindruck, dass die Standards recht unkonkret bleiben oder oftmals so umfangreich sind, dass sie schnell als unpraktikabel zur Seite gelegt werden.

Dennoch sollte man den Wert solcher Standards nicht unterschätzen. Sie bieten oftmals einen reichen Schatz an bedenkenswerten Aspekten und somit auch eine gute Orientierung. Allerdings muss man sie bezüglich der eigenen Situation, Aufgabenstellung und aktuellen Entwicklung interpretieren.

---

[1] Die Abkürzung „ISO“ leitet sich übrigens vom griechischen Begriff „isos“ ab, der soviel wie „gleich“ bedeutet. Einige der nachfolgend dargestellten ISO Normen wurden gemeinsam mit der IEC (Internationale Elektrotechnische Kommission) entwickelt. Aus Vereinfachungsgründen wird im Folgenden auf die Doppelnennung ISO/IEC verzichtet.

[2] Im August 2012 wurde ich im Rahmen meines Engagements in der Fachgruppe Cloud Computing der ISACA durch unser nationales Chapter eingeladen, den Workingdraft der ISO 27017 zu Cloud Computing zu kommentieren. Damals lief die Initiative bereits einige Zeit. Letztendlich wurde der Standard im Dezember 2015 veröffentlicht. Die national begrenzte Norm „Management von Cloud Computing in KMU“ des Deutschen Instituts für Normung (DIN), zu der ich ebenfalls beitragen durfte, schaffte die Publikation immerhin in 14 Monaten.

3. ZENTRALE DEFINITIONEN UND BEGRIFFE

Cloud: Beim zentralen Begriff Cloud wird häufig auf eine Definition des NIST (National Institute of Standards and Technology des US Wirtschaftsministeriums) zurückgegriffen, dessen Übersetzung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) wie folgt lautet.

„Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider- Interaktion zur Verfügung gestellt werden können."

Charakterisiert wird dieser Service laut NIST-Definition durch:

1. **On-demand Self Service:** Die Provisionierung der Ressourcen läuft automatisch ohne Interaktion mit dem Service Provider ab.
2. **Broad Network Access:** Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
3. **Resource Pooling:** Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
4. **Rapid Elasticity:** Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
5. **Measured Services:** Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Vereinfacht ausgedrückt geht es für die Anwender im Kern um die bequeme Nutzung Internet-gestützter Services, möglichst ohne sich um die darunterliegende Technologie kümmern zu müssen. Für die Anbieterseite – worunter sowohl originäre Anbieter als auch IT-Abteilungen zu zählen sind -geht es darum, die Komponenten so zu Services aufzubereiten, dass der Anwender seine Services bequem, sicher, verlässlich und effizient zur Verfügung gestellt bekommt.

Deployment-Modelle

IaaS – Infrastructure as a Service

IaaS sind Infrastruktur-Services, im Sinne bereitgestellter Hardware-Ressourcen wie Prozessoren, Speicher, Netzwerkinfrastruktur und andere grundlegende IT-Ressourcen. Die Art der Nutzung obliegt dabei dem Nutzer.

PaaS – Platform as a Service

PaaS sind Services-Bündel, im Sinne von Infrastruktur-Services sowie Betriebssystemen, Programmiersprachen, Bibliotheken, Datenbanken, Applikations-Servern und Software-Werkzeugen. Der Nutzer hat die Möglichkeit die Service-Bündel zu orchestrieren und hinsichtlich der Nutzung zu konfigurieren. Die konkrete darauf aufsetzende Nutzung obliegt dem Nutzer.

IPaaS – Integration Platform as a Service

IPaaS sind Services, die es ermöglichen, verschiedene Cloud- und „On-Premise-“ Infrastruktur- und Platform-Services Organisations-übergreifend zu kombinieren bzw. zu integrieren.

SaaS – Software as a Service

SaaS sind Anwendungen, die über das Internet nach Bedarf genutzt werden können, wobei die eigentliche Anwendung in der Cloud läuft. Der Nutzer greift mittels Webbrowser oder über spezielle Schnittstellen auf den Service zu. Anpassungen sind nur im Rahmen des Anwendungs-Customizings möglich.

Public Cloud

Public Cloud bezeichnet eine Cloud-Infrastruktur, die öffentlich zugänglich ist (Internet) und deren Services mit anderen geteilt genutzt werden (Multi-Mandanten- bzw. Multi-Tenancy-Architektur). Der Speicherort ist damit üblicherweise nur logisch, aber nicht physisch separiert.

Private Cloud

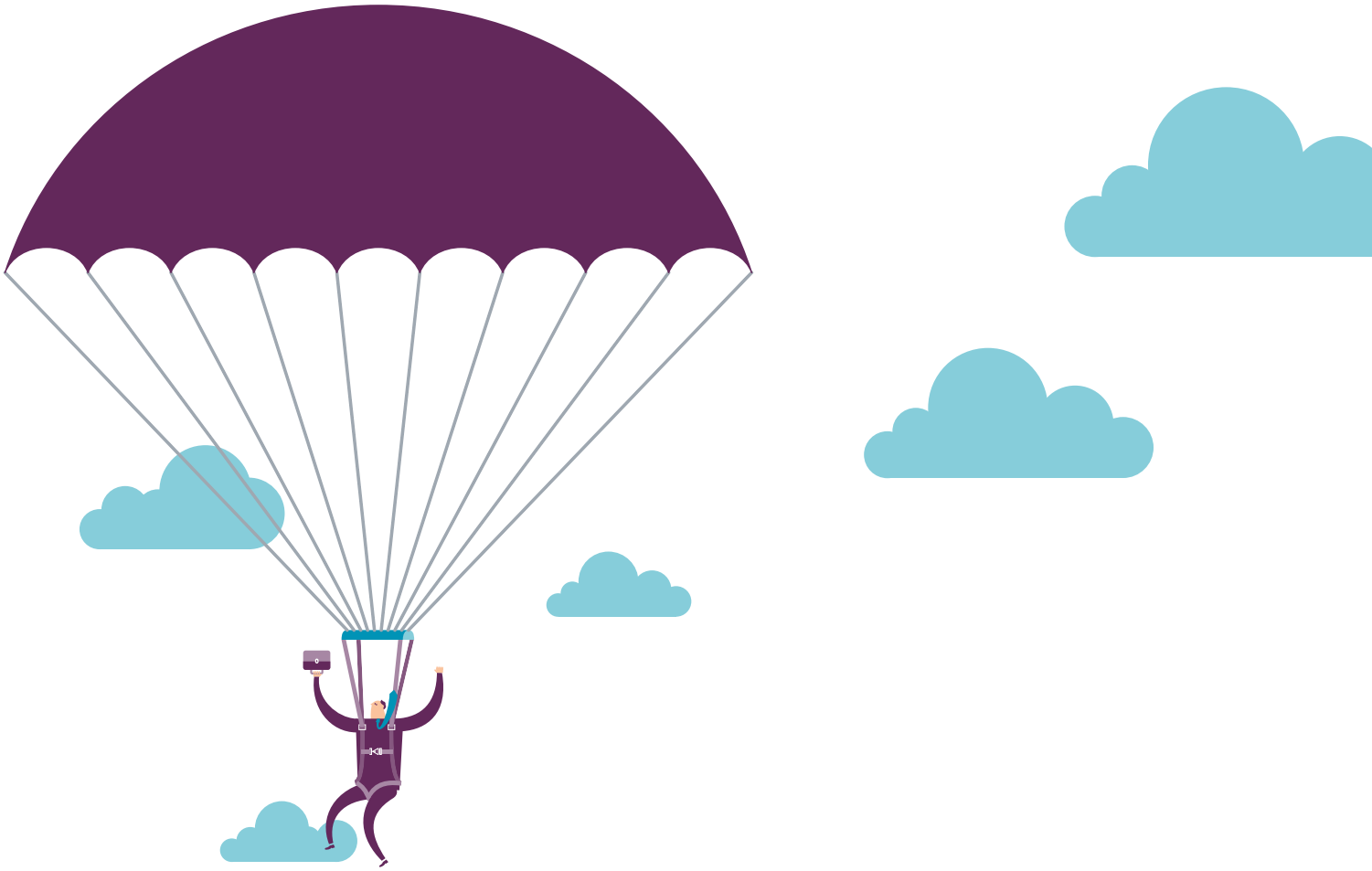
Im Gegensatz zur Public Cloud ist die Private Cloud weitestgehend[3] auch physisch für die ausschließliche Verwendung durch eine einzige Organisation separiert.

Hybrid – Cloud

Hybrid bezeichnet der Verbindung von Private Clouds und Public Clouds.

---

[3] In wie weit bei einem Betrieb von Private Clouds durch Dienstleister auch Rechenzentrums-Komponenten (z. B. Router, Switches etc.) Kunden-dediziert zur Verfügung stehen müssen hängt ggf. von den spezifischen Sicherheitsbedürfnissen des Kunden ab.



Standard: Als Standard wird jede Art von beschriebener Norm bezeichnet. Dabei ist es unerheblich, ob es sich um einen technischen oder organisatorischen Standard handelt.

Virtualisierung: Die Grundidee der Virtualisierung ist es, physische Ressourcen aus einem Ressourcenpool nur dann zu nutzen, wenn sie tatsächlich gebraucht werden. Sie werden bei Bedarf zugewiesen, verhalten sich dann wie eine exklusive Komponente und werden nach Gebrauch wieder freigegeben. Paketierungen von Ressourcen-Bündeln werden teilweise auch als „Container“ bezeichnet.

Prinzipiell sind Virtualisierungen aller physischen Komponenten denkbar, die von Software angesteuert bzw. genutzt werden. Eine Anwendung hat also beispielsweise keinen fest zugewiesenen Rechner mit Prozessor und Speicherplatz mehr, sondern bekommt die erforderlichen Ressourcen zum Zeitpunkt des Bedarfs aus einem großen Pool von Prozessoren und Speicherplatz temporär zugewiesen. Der Rechner ist in der angefragten Form nicht mehr ein dediziertes physisches Gerät, sondern wird nur noch virtuell „vorgegaukelt“. Virtualisierung wird auch im normalen Rechenzentrumsbetrieb eingesetzt. Im Sinne der Zielsetzung vieler Cloud Angebote, Ressourcen „im Hintergrund“ möglichst optimal zu organisieren und per Software zu steuern, sind Virtualisierungstechniken dennoch eine Basistechnologie für Clouds.

4. STANDARDS UND DIE ERWARTUNGEN AN CLOUD-COMPUTING

Erwartungen an Cloud Angebote

Der Begriff der Cloud wird im wahrsten Sinne des Wortes häufig sehr wolkig gebraucht. Hinter dem Begriff „Cloud“ = „Wolke“ steht die Erwartungshaltung, dass der Nutzer eine Leistung von irgendwo aus der Wolke bezieht. Von wo genau, spielt keine Rolle. Vergleichbar dem Strom aus der Steckdose, gibt es nur den definierten Einstiegspunkt, von dem aus der Kunde seine Leistung in Empfang nimmt. Die Webadresse dient quasi als Steckdose. Alles andere wird von den Anbietern im Hintergrund organisiert. In Hinblick auf die immer weiter wachsende Komplexität der Informationstechnologie, die zu beherrschen für die meisten Firmen eine immer schwerer zu stemmende Last darstellt, ist eine solche Vereinfachung eine äußerst verlockende Aussicht.

Aus Unternehmenssicht sind daher die Erwartungen groß, durch die Reduzierung der Komplexität, eigene Aufwende erheblich senken und damit Kosten sparen zu können. Für die wenigsten Unternehmen stellt die Bereitstellung von IT-Leistungen eine Kernkompetenz dar. Zudem werden überwiegend fremdproduzierte Komponenten betrieben. Warum also nicht alles in die Hände von Experten geben, die durch Multiplikation der Leistungen auch erhebliche Skaleneffekte und damit günstigere Preise erreichen können?

Aktuelle Studien belegen, das erwartete Kosteneinsparungen mit Abstand der wichtigste Grund für den Wechsel in die Cloud sind. Erst danach folgen Flexibilitäts- und Transparenz-Erwägungen.

Bedenken gegen Cloud Angebote

Kritiker bemängeln zu Recht, dass Outsourcing im Allgemeinen und Cloud-Services im Speziellen die Abhängigkeit von Dritten erhöht. Abhängigkeiten gibt es jedoch immer: von Software-Anbietern allgemein wie auch von Mitarbeitern mit besonderer Expertise. Abhängigkeiten so zu begrenzen, dass diese keine untragbaren Schäden erzeugen, ist eine allgemeine Managementaufgabe. Clouds sind in dieser Hinsicht keine Besonderheit. Sie haben allerdings ein spezifisches Risiko-Profil, das es zu berücksichtigen gilt. Auch hier kommen Standards wieder ins Spiel. Vertrauen ist schön und an vielen Stellen auch unvermeidlich. Blindes Vertrauen ist manchmal leider auch naiv und provoziert unter Umständen auch Nachlässigkeiten. Gefordert sind also angemessene Kontrollen – dies um so mehr, wenn man gegenüber Dritten verantwortlich ist und sich für die eigenen Entscheidungen zu rechtfertigen hat.

Kontrollen erfordern immer den Vergleich zwischen SOLL und IST. Die Definition des SOLL ist in einer komplexen Umgebung ein aufwendiges Unterfangen und erfordert exzellentes Know-how. Den Aufbau dieses Know-hows will man jedoch gerade vermeiden. Hier helfen Standards, die von Experten definiert wurden und das SOLL zur Verfügung stellen, gegen das geprüft werden kann. In vielen Situationen ist es zudem angemessen, die Prüfung einer unabhängigen Prüfinstanz zu übergeben, die die angemessene Einhaltung des SOLL bestätigen kann oder auch auf Defizite aufmerksam macht.

Standards verbessern das Angebot

Um das Beispiel des Strommarktes nochmals aufzugreifen: Erst die Standardisierung von Netz-Spannung und Steckern ermöglicht es den Herstellern von Elektrogeräten, Ihre Produkte zu günstigen Preisen anzubieten – zum großen Vorteil der Gerätenutzer. Standard sind typischerweise Treiber vielfältiger und günstiger Angebote. Natürlich neigen große Anbieter dazu, Standards zu setzen, so dass es zu Wettbewerbssituationen zwischen Standards kommt: Betriebssysteme sind ein typisches Beispiel dafür. Aber alleine schon die Reduzierung auf wenige Standards hilft Anbietern, Ihre Entwicklungskapazitäten so zu bündeln, das wirtschaftlich attraktive Angebote möglich werden.

5. UNIVERSAL-STANDARDS

Viele Kunden, die sich nicht im Detail mit einzelnen Disziplinen und der Auswahl relevanter Standards auseinandersetzen möchten, wünschen sich häufig ein universelles Zertifikat, das nicht nur Datenschutz oder die technische Sicherheit betrachtet, sondern auch Themen, wie etwa Organisationssicherheit, Verträge, Marktrelevanz oder Compliance umfasst. Umgekehrt ist es für Anbieter verlockend mit einem solchen Universalzertifikat zu werben. Nicht zuletzt versprechen sich Auditoren von solchen Zertifikaten einen steten Strom von Mandaten. Deshalb gab und gibt es diverse Ansätze für solche Zertifikate aus den verschiedenen Bereichen. Nur wenige haben sich allerdings durchgesetzt.

Universalität bedeutet ein sehr umfassendes Betrachtungsspektrum. Dieses tatsächlich zu prüfen oder prüfen zu lassen, ist für die meisten Anbieter nicht wirtschaftlich. Deshalb lautet der Kompromiss zumeist die Betrachtung der Zertifikate Dritter, einfacher Indikatoren und häufig auch der Selbstauskunft der Anbieter.

Dennoch können solche Universalzertifikate hilfreich für eine Vorqualifizierung von Anbietern sein. Bezüglich der spezifischen Situation, insbesondere in Hinblick auf Datenschutz und besondere Sicherheitsanforderungen, sollte jedoch immer geprüft werden, ob und ggf. welche Zertifizierungen ggf. ergänzend erwartet und detaillierter geprüft werden sollten. Anbieter von Universalzertifikaten mit Potenzial sind aktuell:

Trust in Cloud

Das Trust in Cloud Zertifikat des Cloud Ecosystems schafft Transparenz über die Themen

- Qualität des Service-Angebots
- Sicherheit/Zuverlässigkeit
- Deutscher Datenschutz
- Vertragsbedingungen
- Qualität der Organisation
- Marktpräsenz
- Innovationsfähigkeit
- Referenzen

Es berücksichtigt die Spezifika von IaaS/PaaS- und SaaS-Angeboten. Zudem können so-genannte Referenzarchitekturen zertifiziert werden, die aus einem SaaS-Angebot und einem dedizierten Infrastruktur-/Plattform-Angebot bestehen. Das Basis-Zertifikat basiert auf einer Selbstauskunft. Beim ergänzenden „certified" Level-Zertifikat, erfolgen spezifische Auditierungen.

Das Zertifikat versteht sich vor allem als Entscheidungshilfe für mittelständische Organisationen in Deutschland. Zudem bietet die enge Zusammenarbeit mit der German Businesscloud ein Forum für die differenzierte Qualifizierung von Anbietern.

skyhigh – enterprise-ready cloud service

Skyhigh, ein US-amerikanischer Sicherheitslösungs-Anbieter, bietet ein Prüfsiegel an, das 21 verschiedene Prüfkriterien umfasst, aus den Bereichen[4].

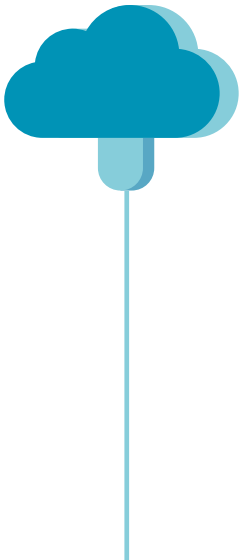
- Datenhandhabung und Verschlüsselung
- Zugriff und Authentifizierung
- Service Sicherheit
- Zuverlässigkeit für Geschäftsbetrieb
- Rechtliche Aspekte

Erwähnenswert ist skyhigh vor allem, weil der Anbieter eine umfassende Anwendungs-Datenbank für mehr als 50 Prüfkriterien für Cloud-Anwendungen aufgebaut hat und diese im Rahmen von Firewall-Monitoring für die Bildung von Warnindikatoren heranzieht. Das in diesem Zuge nunmehr auch ein Zertifikat angeboten wird, ist naheliegend. Er ist amerikanisch geprägt und deshalb hinsichtlich deutscher Datenschutzaspekte wenig aussagefähig. Mit größerer Marktdurchdringung in Deutschland sowie für internationale Anbieter kann ein positives „Listing" oder ein entsprechendes Zertifikat hilfreich sein.

Netskope – cloud due dillegence

Einen ähnlichen Ansatz verfolgt auch Netskope, ebenfalls ein US-amerikanischer Sicherheits-lösungs-Lieferant. Er bietet zwar derzeit kein Prüfsiegel an, pflegt aber ebenfalls eine Daten-bank, in der nach eigenen Angaben mehr als 10.000 Applikationen in sieben Betrachtungs-feldern geprüft wurden. Diese sind frei übersetzt:

- Sicherheit
- Auditierungen/Zertifikate
- Rechtliche Aspekte
- Service Level Agreements
- Verwundbarkeit/Sicherheitslücken
- Wirtschaftliche Stabilität
- Datenschutz



[4] Die Überschriften sind entsprechend der Prüfkriterien ins Deutsche übersetzt, da die englischen Originalüberschriften nur wenig Aussagekraft haben.

6. FUNKTIONALE STANDARDS

SLA

Service Level sollen die erwarteten bzw. zu liefernden Leistungen nachvollziehbar (messbar!) fixieren. Die notwendigen Anforderungen sind abhängig vom konkreten Geschäfts- bzw. Nutzungsmodell. Da die Cloud-Anbieter in der Regel Ihre Leistungen verschiedenen Kunden zur Verfügung stellen und keine kundenspezifischen Service-Level anbieten, muss der Nutzer prüfen, ob das jeweilige Angebot seinen Anforderungen genügt.

Aktuelle Standards zu Service-Leveln beziehen sich typischerweise entweder auf gut vergleichbare Parameter von Infrastrukturen (Verfügbarkeit bzw. max. Ausfallzeiten, Datendurchsatz, Fehlertoleranz, Energie-Effizienz etc.) oder sie begnügen sich mit der Standardisierung von Leistungsklassen.

Verbreitet sind derzeit vor allem Verfügbarkeits-Zertifizierungen für Rechenzentren.

Die Telecommunications Industry Association veröffentlicht und aktualisiert seit 2005 in Kooperation mit der ANSI[5] einen Standard für Telekommunikations-Infrastruktur bzw. dafür eingesetzte Rechenzentren und klassifiziert in ihr vier unterschiedliche Verfügbarkeits- und Sicherheits-Stufen (Tiers genannt)[6].

Unabhängig von der ANSI/TIA-942-Standard, hat das UptimeInstitute®[7], ein amerikanisches Beratungs- und Zertifizierungsunternehmen, eigene vier „Tiers“ definiert. Es hat international eine relativ breite Akzeptanz gefunden – nach eigenen Angaben wurden 567 Zertifizierungen in 66 Ländern durchgeführt.

Das EuroCloud Star Audit-Programm verwendet einen Prüfungsprozess in 5 Stufen. Mit ca. 30 Zertifizierungen bei rund 20 Kunden[8] ist die Verbreitung allerdings noch eher bescheiden. EuroCloud sieht sich als Verband und agiert als in Luxemburg eingetragene Non-Profit-Organisation. Sie steht europäischen Partnerorganisationen offen. Ihre Struktur ist allerdings nicht transparent.[9]

---

[5] American National Standards Institute
[6] http://www.tiaonline.org/standards/tia-standards-overview
[7] https://uptimeinstitute.com/consulting-certification/overview
[8] Nach Angaben der eigenen Webseite, Stand April 2015
[9] https://eurocloud-staraudit.eu/de.html 5 American National Standards Institute

Hinsichtlich der Standardisierung von Leistungsklassen gab es im Juni 2014 einen Vorstoß der EU-Kommission unter der Bezeichnung Cloud Service Level Agreement Standardisation Guidelines *(http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines)*. Sie beschränkt sich allerdings auf die Bezeichnung und Erklärung relevanter Klassen. Best Practice Standards lassen sich daraus leider nicht ableiten.

Authentifizierung

Da fast alle Authentifizierungs-Technologien verschiedene Eigenschaften und damit verbundene Vor-und Nachteile haben, werden oftmals Sicherheitsfunktionen miteinander kombiniert (häufig Two-Factor- oder Multi-Factor-Authentifizierung). Zudem lösen sie unterschiedliche Aufgabenstellungen. Die nachfolgenden Methoden sind daher häufig nur eine Komponente in der konkreten Authentifizierungsstrategie.

OpenID ist ein offener und international weit verbreiteter Authentifizierungs-Standard für die Authentifizierung von Nutzern webbasierter Dienste, der auch von vielen Branchengrößen unterstützt wird (z. B. Facebook, Google, Xing).

Der Service erlaubt es Service Providern mit geringem Aufwand, selber als OpenID Anbieter zu fungieren. Der Benutzer erhält mit der erstmaligen Anmeldung eine URL als Identifier, die es ihm erlaubt, sich bei allen unterstützenden Websites anzumelden. Aufgrund teils proprietärer Implementierungen (z. B. Google) sind nicht alle OpenID- Services zueinander kompatibel.

Microsoft Konto/Microsoft Account

Microsoft bietet seit 1999 einen Single-Sign-On-Service an, der unter verschiedenen Namen geführt wurde (insbesondere Microsoft Wallet, Microsoft Passport. NET Passport, Microsoft Passport-Netzwerk, Windows Live ID). Die aktuelle Bezeichnung ist Microsoft Account bzw. in der deutschen Übersetzung Microsoft Konto. Die Protokolle sind proprietär. Geschätzt werden mehr als 250 Millionen registrierte Benutzer.

SAML

SAML (Security Assertion Markup Language) ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen. Die meisten Browser- bzw. HTML-basierten Anmelde-Implementierungen setzen SAML ein.

OAuth2

OAuth2 ist ein offenes Protokoll, mit dem Anspruch eine standardisierte, sichere API-Autorisierung für Desktop-, Web- und Mobile-Applikationen zur Verfügung zu stellen. Es ist methodisch OpenID ähnlich, wird allerdings in der Regel für den Zugriff auf Ressourcen eingesetzt, wie bspw. bei der Berechtigungsprüfung für verlinkte Dokumente.

Service Orchestrierung

Aus technischer Sicht stellt die Steuerung der Ressourcen eine Schlüsselaufgabe dar. Diese kann sich auf die unterschiedlichen Deployment-Modelle, (IaaS, PaaS, SaaS, IPaaS, Hybrid), auf die Komponenten einzelner Hersteller oder aber auch all diese Ebenen integrierend beziehen. Aufgrund der Vielzahl möglicher Komponenten spricht man mittlerweile häufig von der „Orchestrierung" der Services oder von „Cloud Manager"-Komponenten.

Verständlicherweise gibt es seitens der Anbieter großer Cloud-Infrastrukturen üblicherweise gute Werkzeuge für die eigenen Leistungsangebote. So gesehen kann man die Management-Komponenten der großen Infrastrukturanbieter, wie Amazon AWS (CloudWatch) EMC/VMWare (vCloud), Microsoft Azure, IBM SoftLayer oder in Deutschland auch ProfitBricks als quasi Standard betrachten.

Um Herstellerunabhängigkeit oder zumindest eine breite Marktunterstützung zu erreichen, gibt es verschiedene OpenSource Projekte. Bedeutsam sind hier vor allem:

OpenStack

OpenStack ist ein freies Architektur-Projekt für Cloud-Architekturen. Es gliedert sich in verschiedene Teilaspekte auf. Schwerpunkt sind das Management von virtuellen Maschinen und Speicher sowie die dafür erforderlichen Verwaltungs- und Kommunikations-Komponenten. OpenStack wird von einer ganzen Reihe namhafter Unternehmen unterstützt und weiter entwickelt, wie z. B. Cisco, Citrix, Dell, Fujitsu, HP, IBM, Ericsson, Hitachi, Huawai, Intel, NEC, NetApp. Nokia, Oracle, rackspace, redhat, SAP, Suse, Symantec, Ubuntu, VMware oder Yahoo[10]. Open Stack gehört damit wohl zu den etabliertesten Cloud Standards überhaupt. Für den Geschäftseinsatz empfehlen sich zusammengestellte Pakete, sogenannte Distributionen, für die die Anbieter auch Support leisten (z. B. HP, RedHat und Suse).

OpenShift

OpenShift wird zu den „Platform-as-a-Service" oder „PaaS" gezählt. Es bietet Steuerungskomponenten für die Orchestrierung von Software-Komponenten, die typischerweise für Web-Applikationen benötigt werden. Zusammengefasst werden beispielsweise Betriebssystem, Datenbank, Web-Application-Server sowie Runtime-Umgebungen für die Programmiersprachen und ergänzende Libraries und Ressourcen. Architektonisch betrachtet ist es damit eine Schicht „näher" an den eigentliche Applikationen. OpenShift läuft in der Regel auf OpenStack-Infrastrukturen und ergänzt diese. Es gibt eine OpenSource Initiative unter der Bezeichnung OpenShift Origin *(http://www.openshift.org/)* sowie professionelle Paketierungen, wie zum Beispiel von RedHat (openshift.com).

[10] https://www.openstack.org/foundation/companies/

Cloud Foundry

Ebenfalls ein Open-Source- PaaS Angebot ist die Cloud Foundry. Ziel der Cloud Foundry ist vor allem die Verteilung, Ausführung und Verwaltung von Anwendungen in Umgebungen mit vielen virtuellen Maschinen. Applikationen, können über Cloud Foundry die benötigten Ressourcen (z. B. Datenbanken, Massaging-Dienste oder ein File-System) über Services nutzen, die sich in der jeweiligen Umgebung zum Teil automatisch konfigurieren lassen. Es wird ebenfalls von vielen namhaften Firmen unterstützt. So ist die Cloud Foundry bspw. Basis für BlueMix von IBM. In der Cloud Foundry Foundation sind u. a. die Firmen Docker, Emc, Ericsson, Fujitsu, HP, Intel, NTT, Toshiba oder VMware vertreten[11].

Opendaylight

Bei Opendaylight handelt es sich um eine Initiative der Linux Foundation. Es handelt sich um ein Open Source Projekt mit dem Ziel, Netzwerkfunktionen zu virtualisieren[12].

Eucalyptus

(Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems): Eukalyptus ist ein Service zur Verwaltung von Rechner-Clustern und wurde originär als lokale Implementierung von Amazon AWS entwickelt.

Geschäfts-nahe Service-Komponenten

Einen Abstraktions-Level über den klassischen Entwicklungs- und Infrastruktur-Management-Frameworks gibt es Lösungen für Geschäfts-nahe Service-Komponenten (z. B. für Abrechnung und Rechnungsstellung, Archivierung, Modell-basierte Entwicklung oder die Cloud-Integration von bestehenden On-Premise Lösungen). Die WebServiceFactory (StoneOne) bietet bspw. in Deutschland bereits seit einigen Jahren verschiedene Komponenten für die schnelle Anwendungsentwicklung Cloud-basierter Lösungen. Große Cloud Entwicklungs-Infrastrukturen, wie sie beispielsweise von Microsoft und IBM angeboten werden, haben allerdings ebenfalls immer komplexere Service-Entwicklungsbausteine im Portfolio und konvergieren zunehmend in dieses Marktsegment.

Applikations-Integration

Auf die Integration von Applikations-Services bzw. verschiedener SaaS-Angebote wird im Kapitel 7 „Marktplätze/App Stores/Service Integration“ näher eingegangen.

---

[11] http://www.cloudfoundry.org/about/index.html

[12] vgl. Begriffe und Definitionen!

Container

Container-Konzepte unterstützen die Verteilung und Skalierung von Anwendungen und spielen daher eine zunehmend bedeutende Rolle. Die große Beliebtheit des noch jungen Pioniers Docker hat jüngst (2014/2015) zu einigen Ergänzungs- und Konkurrenzangeboten geführt. Neuester Trend ist das Open Container Project, das sich zum Ziel gesetzt hat, einen „Standard-Container“ zu entwickeln.

Docker

Docker nutzt Container als Virtualisierungstechnik im Kontext von Linux Betriebssystemen, die sich leicht paketieren und transferieren lassen. Diese Grundeigenschaft zusammen mit der Möglichkeit vordefinierte Filesysteme zu vererben und dem mittlerweile umfangreichen Katalog vordefinierter Docker-Container haben zu einer großen Beliebtheit von Docker geführt.
Es ist seit 2013 auf dem Markt.

Ubuntu LXD

Ubuntu LXD kann als Ergänzung zu Docker angesehen werden. Es hat den Anspruch die Vorteile der einfach distribuierbaren Container mit der Abschottung/Sicherheit und Hardware-Unterstützung einer Virtualisierungsumgebung zu verbinden.

Rocket CoreOS

Bei Rocket CoreOS handelt es sich entwicklungsgeschichtlich quasi um einen „Seitenstrang“ zu Docker, der dem Anspruch folgt, eine noch einfachere, im wesentlichen auf die Abbilder, eine Laufzeit-Umgebung und Möglichkeiten zum Auffinden von Containern reduzierte Distribution.

Photon:

Photon ist eines von mehreren Open Source Projekten von VMWARE. Es handelt sich dabei um ein schlankes Linux-Betriebssystem, dass in der Lage sein soll, Container und virtuelle Maschinen nativ auf einer einzigen Plattform zu betreiben.

Open Container Project

Unter dem Dach der Linux Foundation haben sich eine ganze Reihe namhafter Firmen zusammengefunden, um einen Standard für Container zu entwickeln. Allen voran hat Docker angekündigt, seine Technik für das Open Container Project zu stiften. Weitere Unterstützer sind zudem CoreOS, Amazon (AWS), Cisco, EMC, Fujitsu, Google, HP, Huawai, IBM, Intel, Microsoft, Pivotal, RedHat und VMware. Zielsetzung ist ein Container-Standard, unabhängig von bestimmten Plattformen, Orchestrierungs-Stacks und Clients. Erste Spezifikationen wurden im Herbst 2015 veröffentlicht.

Cloud Native Computing Foundation (CNCF)

Eine andere breiter unterstützte Initiative hat sich im Sommer 2015 zur Cloud Native Computing Foundation (CNCF) formiert, die ebenfalls die Verwaltung von Containern standardisieren möchte. In diese wurde insbesondere Kubernetes von Google eingebracht. In ihr versammeln sich bekannte Firmen wie z. B. AT&T, Box, Cisco, Cloud Foundry Foundation, CoreOS, Cycle Computing, Docker, eBay, Goldman Sachs, Google, Huawei, IBM, Intel, Mesosphere, RedHat, Twitter, und VMware.

Machine-to-machine (M2M)

Die Organization for the Advancement of Structured Information Standards (OASIS) standardisiert seit 2013 **MQTT (Message Queue Telemetry Transport)** als offenes „Protokoll des Internets der Dinge“. Es ist spezialisiert auf die Kommunikation mit Sensoren, Aktoren, Smart-Devices oder eingebetteten Systemen, die gegebenenfalls auch über sehr beschränkte Kommunikations-Kanäle interagieren sollen.

Daneben versuchen diverse Anbieter Standards entweder alleine und im Rahmen kooperativer Allianzen zu schmieden. Fast alle Schwergewichte sind in der einen oder anderen Form mit dabei: Industriegiganten wie Siemens, GE und Bosch treiben Ihre Standards ebenso wie die großen IT-Anbieter Amazon, Google, IBM, SAP, Intel und Cisco. Dazu gesellen sich erfolgreiche Nieschenanbieter wie beispielsweise Jasper oder PTC. Klare Trends oder dominante Marktführer sind derzeit jedoch noch nicht erkennbar.

Skalierung

Eine wichtige Eigenschaft von IaaS und PaaS-Angeboten ist die Skalierbarkeit. Kern der Funktionalitäten ist daher das Management von Anwendungen und Komponenten auf Rechner-Clustern. Das JAVA basierte Framework **Hadoop** ist der am weitesten verbreitete de facto-Standard. Alternativen könnten sich allerdings aufgrund der Initiativen von **Mesos** (Apache) und OpenStack ergeben.

Prozessintegrationsstandards

Von der Vision, Arbeitspakete mühelos durch die Anwendungen verschiedener Hersteller durchschleusen zu können, ist die Praxis leider noch weit entfernt. Es dominieren derzeit noch die individuellen Schnittstellen. In den zurückliegenden Jahren gab es zwar immer wieder Initiativen, Prozessmodellierung zu standardisieren und über Systeme austauschbar zu machen. Der große Durchbruch steht aber leider immer noch aus. Dies mag zum Teil an der Verschiedenheit und Komplexität der unterschiedlichen Anwendungssysteme liegen.
Des Weiteren zielten die Bemühungen gleich auf zwei unterschiedliche Ebenen, nämlich die Prozessmodellierung (Design) auf der einen Seite und die maschinelle Lesbarmachung (Verarbeitung) auf der anderen Seite. Und nicht zuletzt geht es häufig auch um das Zusammenführen verschiedener Services, worauf im Abschnitt 8 unter „Integrierte Services“ noch näher eingegangen wird.

BPMN

Am vielversprechendsten erscheint zum gegenwärtigen Zeitpunkt BPMN als Modellierungssprache, die es sogar geschafft hat, als ISO-Norm internationale Anerkennung zu finden (ISO/IEC 19510). Zudem erlauben es verschiedene Workflow-Engines, BPMN-Modelle direkt auszuführen. Die Stärken von BPMN liegen allerdings eher in der Modellierung von Geschäftsprozessen mit Benutzer-Interaktionen und weniger in der technischen Integration verschiedener Anwendungssysteme. Dieses Defizit kann allerdings durch die Kombination mit entsprechenden Integrations-Services (BPEL-basierte Systeme oder BPMN-fähigen Enterprise-Services-Bus-Systeme) ausgeglichen werden.

XPDL

XML Process Definition Language (XPDL)[13], ist eine maschinell auswertbare Prozessbeschreibungssprache, die mit der BPMN Spezifikation kompatibel ist. XPDL ist graphenorientiert und damit auch methodisch nah an der Modellierung von Geschäftsprozessen durch BPMN. Nicht zuletzt weil die Workflow-Engine-Anbieter BPMN häufig direkt interpretieren, ist ein flächiger Durchbruch des Standards eher fraglich.

BPEL

Eine weitere Prozessausführungssprache ist BPEL (Business Process Execution Language). Die Zielrichtung von BPEL ist eher die Orchestrierung von Computerprogrammen, über Webserviceaufrufe. Damit hat BPEL vielleicht das Potenzial, die technischen Integrations-Defizite von BPMN zu schließen.

Sicherheitsstandards

Sicherheit – das große Thema für Cloud Services.

ISO 270xx

Die ISO beschäftigt sich schon seit Jahren mit Methoden der IT-Sicherheit. Alle diese Normen beginnen mit der 270 gefolgt von zwei Stellen. Im Zentrum steht die ISO 27001, die für das Sicherheits-Management-System steht. Doch der Vollständigkeit-halber hier eine kurze Aufstellung wichtiger begleitender Standards der 27000 Reihe, die allesamt unter dem Überbegriff „Information technology – Security techniques“ veröffentlich wurden, auf die aber im Folgenden nicht detaillierter eingegangen wird. Diese sind

27000 Information security management systems – Overview and vocabulary
27001 Information security management systems – Requirements
27002 Code of practice for information security management
27003 Information security management system implementation guidance
27004 Information security management – Measurement

[13] Seit 1993 in Normung seitens der Workflow Management Coalition (WfMC)

27006 Guidelines for information security management systems auditing
27010 Information security management for inter-sector and inter-organizational communications
27032 Guidelines for cybersecurity
27033 Network security
27036 Information security for supplier relationships

Speziell für das Thema Cloud Computing, sind darüber hinaus folgende Normen:

27017 „Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002". Sie ist als Ergänzung zur 27002 aufgesetzt und kommentiert diese in Hinblick auf Cloud-spezifische Ergänzungen.

27036-5 – Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services. Die Einbindung von Sub-Lieferanten in das Sicherheitssystem des Unternehmens wurde bereits durch 3 Teile (Parts) durch die ISO aufgegriffen. Ein geplanter vierter Teil soll den Besonderheiten der Cloud gerecht werden.

CSA

International ist die „Security Guidance for Critical Areas of Focus in Cloud Computing der Cloud Security Alliance (CSA) hervorzuheben. Sie ist hinsichtlich der Governance und Compliance-Ausführungen zwar etwas US-fokussiert, bietet jedoch fundierte Darstellungen über alle wichtigen Themenbereiche, die mit Cloud Security zu tun haben. Dieses vielleicht auf den ersten Blick sehr umfassend wirkende Werk stellt in der Version 3 neben den Herausforderungen auch Hintergründe und Lösungsansätze technisch detailliert dar, ohne in Bits und Bytes abzudriften. Außerdem bietet die CSA Excel-basierte Arbeitshilfen und Checklisten an, die für das Mapping zu anderen Standards oder etwaige Evaluationen eine gute Grundlage bieten können.

BSI

National und insbesondere für öffentliche Organisationen bedeutsam sind die Empfehlungen des Bundesamtes für Informationssicherheit (BSI). Neben einer Reihe nützlicher Informationsdokumente gibt es einen eigenen umfassenden Baustein (B 1.17 Cloud-Nutzung[14]) im Grundschutzkatalog. Er behandelt umfassen verschiedene Bedrohungsszenarien und thematisiert eine ganze Reihe von Maßnahmen für die Einführung und die Nutzung von Clouds. Die Maßnahmen sind eher „Sicherheits-lastig". Zudem besteht die Gefahr, dass die diversen Querverweise zu anderen Grundschutz-Einträgen bei „Nicht-BSI-Grundschutz-Erfahrenen" mehr Fragen aufwerfen als Antworten geben. Eine weitgehende Orientierung am BSI Grundschutzkatalog ist daher ein ambitioniertes und aufwendiges Vorhaben.

[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Cloud_Nutzung/Baustein-Cloud-Nutzung-B1_17.pdf?__blob=publicationFile

Im Dezember 2015 wurde zudem der Entwurf eines Kriterienkatalogs vorgestellt, der Grundlage für eine Sicherheits-Testierung von Cloud-Anbietern bilden soll. Er stützt sich vor allem auf international anerkannten Sicherheitsstandards ISO 27001/27002, CSA Cloud Control Matrix, AICPA Trust Service Principles, IDW ERS FAIT 5 sowie den eigenen Veröffentlichungen zum IT Grundschutz und zu SaaS Sicherheitsprofilen ab und stellt in einer Referenzierungsmatrix die Gemeinsamkeiten dar. Geplant sind Testate, die sich vergleichbar mit einer Bilanzprüfung, auf zurückliegende Prüfungszeiträume beziehen werden. Obwohl bestehende Zertifikate berücksichtigt werden können, dürfte mit der Zertifizierung ein signifikanter Validierungsaufwand verbunden sein. Noch ist unklar, wer mit welcher Akkreditierung die als Ergebnis angestrebten Testate wird abnehmen dürfen.

SOC-2/SOC-3

SOC ist eine Gruppe US-amerikanischer Reporting-Standards. Sie werden herausgegeben von AICPA[15] der Vereinigung der Wirtschaftsprüfer in den USA (vergleichbar dem IDW[16] in Deutschland). Sie bilden die Grundlage für die Prüfung und Bestätigung der Verfügbarkeit eines funktionierenden Kontrollsystems von Dienstleistern (daher die Abkürzung SOC: **S**ervice **O**rganization **C**ontrols). An US-Börsen-gelisteten Unternehmen helfen diese Prüfungsstandards, den Kontrollpflichten gegenüber eingesetzten Dienstleistern Compliance-gerecht nachzukommen.

Für das Thema Cloud ist der SOC-2 von besonderem Interesse. Er adressiert vor allem IT-Outsourcing-Anbieter und Shared Service-Center, die Rechenzentren betreiben, da vor allem Kontrollen in Bezug auf Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und Datenschutz geprüft werden. Wer also in den USA Kunden mit seinen Lösungen versorgen möchte, sollte sich nicht über etwaige Zertifizierungsnachfragen entsprechend SOC-2 wundern. Der detaillierte Prüfungsbericht wird auf Anfrage und nur mit Zustimmung des Geprüften zur Verfügung gestellt.

Der SOC-3 ist inhaltlich vergleichbar dem SOC-2. Er geht jedoch nicht auf einzelne Prüfungsschritte und deren Ergebnisse ein, sondern bestätigt stark aggregiert die Prüfung, so dass er einem breiteren Interessentenkreis zur Verfügung gestellt werden kann.

BMWI TCDP (Trusted Cloud Datenschutzprofil)

Das Bundesministerium für Wirtschaft und Energie (BMWI) hat im Rahmen seiner Initiative Trusted Cloud eine eigene Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ eingesetzt. Im Ergebnis wurden verschiedene Arbeits- und Thesenpapiere entwickelt. Von besonderer Bedeutung für die Standardisierung sind vor allem zwei Aspekte: das Trusted Cloud Datenschutzprofil sowie Schutzklassen in der Datenschutzzertifizierung.

---

[15] American Institute of Certified Public Accountants

[16] Institut der Wirtschaftsprüfer

TCDP

Das Trusted Cloud Datenschutzprofil soll die Grundlage bilden, für das Ziel, einen Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten zu etablieren. Auch wenn bislang noch die rechtliche Umsetzung der Thesenpapiere fehlt, besteht doch eine gewisse Wahrscheinlichkeit, dass entsprechende gesetzliche Rahmenbedingungen in enger Anlehnung an die Thesenpapiere folgen.

Schutzklassen

Hinsichtlich des Schutzbedarfs für bestimmte Datenklassen gibt es neben gesetzlichen Vorgaben aus dem Datenschutz [17] noch keine Standards, die sich am Markt durchgesetzt haben. Vorgestellt wurde allerdings im Rahmen der Trusted Cloud-Initiative des Bundesministeriums für Wirtschaft und Energie ein Leitfaden für Schutzbedarfsklassen (Schutzklassen in der Datenschutz-Zertifizierung). In Verbindung mit dem TCDP soll damit eine adäquate Zertifizierung für unterschiedliche Zwecke in Hinblick auf die mögliche Verarbeitung personenbezogener Daten konform zu datenschutzrechtlichen Anforderungen ermöglicht werden.

Sicherheits-Komponenten-Standards

Verschlüsselung

Cloud-spezifisch Verschlüsselungs-Algorithmen sind derzeit nicht zu erkennen. Die Wahl geeigneter Verfahren hängt derzeit überwiegend vom Deployment-Modell und der abzusichernden Architektur-Komponente ab (Übertragung zum Cloud-Provider, Zugriff auf die Provider-Infrastruktur, Speicherung, Verarbeitung etc.). Dabei wird auf bewährten Verschlüsselungs-Technologien (PKI, Tokenization, Advanced Encryption Standard/AES etc.) zurückgegriffen.

Während die Übertragung und Speicherung von Daten in Infrastrukturen mit aktuellen Verschlüsselungsverfahren allgemein als hinreichend sicher gelöst angesehen werden, stellt die Verarbeitung von Daten bislang ein praktisch ungelöstes Problem dar. Zwar gibt es Verfahren für Rechenoperationen auf verschlüsselten Daten, diese sind aber extrem rechenintensiv und in praktischen Entwicklungsumgebungen nicht verfügbar. Deshalb haben sie auch keine praktische Relevanz. Bei der Verarbeitung von Daten in der Cloud, müssen also die Umgebungsbedingungen für den Schutzbedarf angemessen ausgestaltet sein.

Schlüsselverwaltung

Es gibt einige allgemeine Standards zur Schlüsselverwaltung, insbesondere:

- OASIS Key Management Interoperability Protocol (KMIP): Protokoll zur Kommunikation zwischen Verschlüsselungssystemen.
- NIST SP 800-57: Richtlinien zur Schlüsselverwaltung und Wiederherstellung sowie empfohlenen Arten von Verschlüsselungsverfahren und Schutzanforderungen.
- ISO/IEC 11770-5: Spezifikationen zum Umgang mit Schlüsseln.

---

[17] Personenbezogene Daten, besondere Daten im Sinne des § 3, Abs 9 BDSG

Hinsichtlich der Verwaltung von Schlüsseln gibt es zwei grundsätzliche Ansätze. Zum einen kann die Strategie verfolgt werden, möglichst alle Schlüssel on-premise zu halten und bspw. über entsprechende High-Security Modules (HSM) abzusichern. Zum anderen bieten einige Hersteller aus dem Security-Umfeld Cloud-basierte Schlüsselverwaltungen an (z. B. Amazon AWS CloudHSM, Symantec PKI Cloud Managed Services, Porticor Virtual Key Management Service etc.). Ein echter Cloud Standard für die Schlüsselverwaltung ist allerdings derzeit noch nicht absehbar.

Exit und Migration

Ein häufiges Argument für die Cloud ist die leichte Austauschbarkeit der Serviceanbieter. Dabei werden die Herausforderungen einer Migration jedoch häufig kaum bedacht.

Soweit nur Verarbeitungskapazitäten dynamisch bzw. temporär gebucht werden, muss für eine Migration nur auf entsprechende Standards der Infrastrukturkomponenten (Betriebssysteme, Prozessoren, Frameworks etc.) und Orchestrierungswerkzeuge geachtet werden. Kommen Daten mit ins Spiel, müssen die Übermittlungsprotokolle und Schnittstellen abgestimmt sein sowie die zu übertragenen Volumina, verfügbaren Bandbreiten oder Speichermedien berücksichtigt werden. Gerade die Übertragung von Datenarchiven kann zu überraschenden Migrationslaufzeiten führen. Die Übertragung von einigen Terabyte Daten kann leicht die verfügbaren Übertragungsbandbreiten sprengen. (Spätestens dann rächt sich blinde Datensammlungswut und fehlende Löschstrategien für den laufenden Betrieb …) Und die Idee, diese Daten „einfach auf ein paar Festplatten zu schreiben und diese zu verschicken“, wirft bei entsprechender Sensibilität der Daten sofort eine ganze Reihe von Sicherheitsfragen auf. Ganz kompliziert wird es, wenn der Service über eigene „Logik“ für die Bildung von Kontext oder die Verarbeitung verfügt. Diese zu übertragen kann an Know-how, an Intellectual Properties des Anbieters (Programmcode) oder Lizenzrechten Dritter scheitern. Nicht zuletzt muss die korrekte Übertragung am Ende validiert werden.

Über die Migration von Daten hinaus, gibt es derzeit nur Beachtungs-Empfehlungen im Rahmen der Vertragsgestaltung (siehe Abschnitt „Verträge“!), aber keine technischen Standards, die im Markt bereits Verbreitung gefunden haben.

7. GOVERNANCE, RISK UND COMPLIANCE

Corporate Governance/Interne Kontrollsysteme (IKS)

Unter Korporale Governance wird die Unternehmens- oder Organisationsführung allgemein verstanden. Auch wenn „Führung“ nicht alleine auf Steuerung reduziert werden darf, bildet Steuerung dennoch eine wesentliche Grundlage für eine gut funktionierende Organisation. Zudem ist sie eng interagierend mit der Unternehmens-Mission also dem eigentlichen Geschäftsmodell und den daraus abgeleiteten Zielen. Soweit Cloud-Anwendungen entweder Träger des Geschäftsmodells oder zumindest wesentliche Beiträge zur Zielerreichung erbringen, müssen sie in das unternehmerische Steuerungsmodell integriert werden.

Für die Steuerung von Unternehmen gibt es verschiedene methodische Ansätze.

Kapitalgesellschaften sind ihren Eigentümern zur Rechenschaft verpflichtet. Spektakulären Pleiten, die auf kriminelle Unternehmensführung zurückzuführen waren, folgte der Ruf nach Kontrollen, die sicherstellen, dass die Ziele des Unternehmens verfolgt werden und Bedrohungen/Risiken frühzeitig erkannt und abgewendet werden. Entsprechende Forderungen sind sowohl international (z. B. SOX) als auch national (z. B. Aktiengesetz, Deutscher Corporate Governance Kodex) in die Gesetzgebung oder „Corporate-Governance“-Standards eingeflossen.

Wie auch immer diese Kontrollen aufgrund der Branche oder Firma konkret ausgeprägt sind, soll sichergestellt werden, dass sie über die verschiedenen Managementebenen systematisch durchgeführt, analysiert und (ggf. aggregiert) weiterberichtet werden. Dieses „System“ wird als Internes Kontrollsystem (IKS) bezeichnet.

Die Kontrollen können von Branche zu Branche und von Unternehmen zu Unternehmen sehr unterschiedlich ausgeprägt sein. Um dennoch die Angemessenheit der Kontrollen möglichst objektiv beurteilen zu können, wurden Kontroll-Prinzipien und Standards entwickelt. Treiber hierfür waren und sind die Berufsverbände der Wirtschaftsprüfer, die ihren Mitgliedern entsprechende Prüfungswerkzeuge und Leitfäden an die Hand geben. Für die zu prüfenden Organisationen macht es natürlich genauso Sinn, sich an diesen Standards zu orientieren.

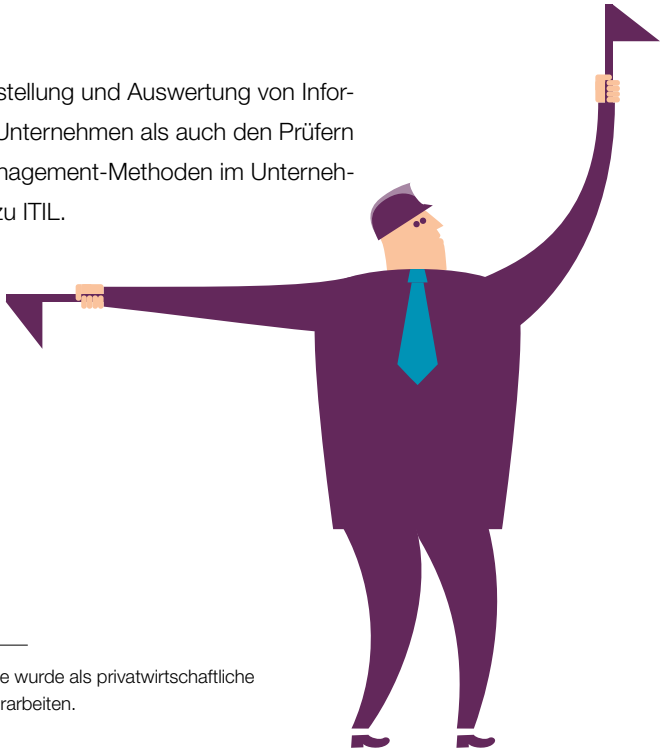
GOVERNANCE
RISK
COMPLIANCE

Für Interne Kontrollsysteme publiziert die COSO[18] bereits seit 1987 Empfehlungen, deren Grundprinzipien bis heute von den meisten renommierten Standards aufgegriffen werden. Ursprünglich vor allem auf die Finanzsysteme gerichtet (COSO I) , erweiterte sich der Fokus mit COSO II auch auf das Enterprise Risk Management (ERM). Entsprechende Prüfungsstandards für Interne Kontrollsysteme hat für Deutschland das IDW herausgebracht. Von besonderer Bedeutung im Zusammenhang mit Cloud-Computing sind dabei der IDW PS 330 zur Prüfung des Einsatzes von Informationstechnologie zur Rechnungslegung sowie der IDW PS 951, der die zusätzlichen Anforderungen an das Interne Kontrollsystem bei Auslagerung (beim auslagernden Unternehmen sowie beim Dienstleistungsunternehmen) im Rahmen der Abschlussprüfung betrifft. Auf die Bedeutung von Prüfungsstandards wird im Abschnitt „Auditierung“ näher eingegangen.

Aufgrund des allgemein zunehmenden Wertbeitrags der IT zu den Geschäftszielen, wurden zur Steuerung der IT verschiedene Standards mit unterschiedlichen Schwerpunkten entwickelt, die bestehende Grundprinzipien (wie bspw. aus COSO) und Kontrollobjekte entsprechend der IT-spezifischen Besonderheiten differenzieren.

Cobit (***C****ontrol* ***O****bjectives for* ***I****nformation and Related* ***T****echnology)*, wird herausgegeben durch den internationalen Verband der IT-Prüfer ISACA (Information Systems Audit and Control Association). Cobit war, wie der Name es andeutet, bis Version 4.1 vor allem eine umfassende Sammlung von Kontrollzielen für die IT. Ausgehend von den Unternehmenszielen und Handlungsprinzipien werden für verschiedene Prozesse der IT Sub-Ziele und Detailprüfungen vorgeschlagen, die wiederum mit einem 6-stufigen Reifegrad-Modell unterstützt werden. Ergänzende Management Guidelines zu Themen wie Wirtschaftlichkeit, Risiko und Sicherheit (ValIT, Risk IT BMIS) wurden in der Version 5.0 zu einem umfassenden Steuerungsrahmenwerk konsolidiert.

Viele Unternehmen orientieren sich an Cobit, da die Bereitstellung und Auswertung von Informationen im Rahmen von Prüfungen (Audits) sowohl den Unternehmen als auch den Prüfern die Arbeit erleichtert. Zur Unterstützung verschiedener Management-Methoden im Unternehmen werden ergänzende Mappings angeboten, wie z. B. zu ITIL.



[18] Committee of Sponsoring Organizations of the Treadway Commission; sie wurde als privatwirtschaftliche Organisation gegründet, um Empfehlungen für Corporate Governance zu erarbeiten.

Best Practices

Zwischen Wunsch und Wirklichkeit liegen oftmals Welten. Und gerade für sogenannte Support-Prozesse im Unternehmen ist Perfektionismus nur selten eine sinnvolle Strategie. Vielmehr geht es in Bezug auf die unterstützenden Services meist darum, für einen günstigen Preis eine marktübliche Leistung einzukaufen. Aber was ist „Markt-üblich"? Hier helfen „Best Practices" aus den Reihen der Betroffenen. In diesem Zusammenhang können die Veröffentlichungen der Open Data Center Alliance (ODCA) hilfreich sein. Der Name der Organisation ist irreführend und wohl der Historie geschuldet. Ursprünglich von Intel initiiert, handelt es sich de facto um eine internationale Anwender-Vereinigung[19] mit dem Ziel, Best Practices für Cloud Computing zu formulieren. Sie publizieren u. a. Nutzungsmodelle für unterschiedliche Anwendungsfälle (IaaS, PaaS, …) sowie für Datensicherheit[20].

IT Service Management (ITSM)

Die IT als Service-Anbieter zu betrachten ist mittlerweile nicht mehr neu. Entsprechend erfreuen sich Service Management Methoden wachsender Beliebtheit in der IT. Hierfür steht vor allem der Begriff ITSM (IT Service Management). International besonders verbreitet ist ITIL (IT Infrastructure Library). Es handelt sich dabei um eine Sammlung von Best Practices, die sich an Geschäftsprozessen orientiert. Eine korrespondierende Norm hat die ISO herausgegeben unter der Bezeichnung ISO 20000 „Information technology – Service management".

Gelegentlich werden im Zuge des Service Managements auch Standards zur Capability Maturity Model Integration (CMMI) und zum Projektmanagement, wie PMBok (Project Management Body of Knowledge) oder Prince2 (Projects in Controlled Environments) angeführt. Mit der gleichen Berechtigung könnte man auch Agile Entwicklung oder SCRUM als Methoden der Software-Entwicklung thematisieren. Diese ohne Zweifel ebenfalls nützlichen Standards bieten in Hinblick auf die Grundidee von Cloud Computing, „Services einfach einzukaufen", jedoch kaum Mehrwert. Deshalb wird auf eine ausführlichere Darstellung an dieser Stelle verzichtet.

Business Continuity Management (BCM)

Beim Business Continuity Management (zu deutsch „Betriebskontinuitätsmanagement") geht es um die Planung und Steuerung der Vermeidung von Betriebsunterbrechungen. Da für viele Cloud-Angebote eine hohe Service-Verlässlichkeit seitens der Nutzer erwartet wird, kommen den Maßnahmen zur Aufrechterhaltung des Betriebs eine besondere Bedeutung zu. BCM kann ein wesentlicher Maßnahmen-Baustein für das Risiko-Management sein (vgl. Kapitel Risiko-Management!).

---

[19] Lt. Wikipedia sind Mitglieder bspw. AT&T, BMW, Capgemini, CERN, China Life, China Unicom Group, Deutsche Bank, eBay, JPMorgan Chase, Lockheed Martin, Logica, Marriott International, Motorola, National Australia Bank, Nokia, Royal Dutch Shell, Terremark, und UBS.

[20] www.opendatacenteralliance.org

Die ISO hat sich auch dieses Themas angenommen und mit der Norm ISO 22301 „Societal security – Business continuity management systems – Requirements“ einen internationalen Standard für die Implementierung eines entsprechenden Maßnahmen-Kataloges publiziert. Eine spezielle Differenzierung für IT wurde ergänzt in Form der ISO 27031 „Guidelines for information and communication technology readiness for business continuity“.

Wirtschaftliche Stabilität

Der Ausfall eines zentralen Serviceanbieters kann sich u. U. verheerend auswirken. Daher spielt neben den Vorkehrungsmaßnahmen für eine effektive Exit-Fähigkeit auch die Beobachtung der wirtschaftlichen Stabilität eine Rolle. Neben dem detaillierten und fachkundigen Studium veröffentlichter Bilanzen, bietet sich auch noch die Möglichkeit, Einschätzungen von Wirtschaftsauskunfteien oder Ratingagenturen einzuholen. Diese betrachten zwar vordergründig nur die Ausfallwahrscheinlichkeiten bzw. Kreditwürdigkeit (Bonität) von Schuldnern, geben aber natürlich einen guten Hinweis auf die Überlebensfähigkeit eines Unternehmens. Zwar ist die grundlegende Kreditwürdigkeit bei kleinen Unternehmen oder innovativen Startup – sofern sie überhaupt bewertet wurden – kein absolutes Messinstrument. Deutliche Verschlechterungen der Bewertung können allerdings ein Hinweis auf mögliche Probleme sein.

Risiko-Management

Jede Entscheidung, die wir für die Zukunft treffen, geht einher mit der Unsicherheit, ob diese auch so eintrifft. Absolute Sicherheit gibt es nicht. Unsere Versuche, die Zukunft durch Rückschau und Prognosen vorherzusehen, sind limitiert durch unsere natürlichen Grenzen, die reale Komplexität messen und verarbeiten zu können. Deshalb scheitern wir immer wieder an unseren vereinfachten Theorien und den daraus geschlossenen Annahmen. Wer über den Moment hinaus Geschäfte machen will, muss dennoch Annahmen treffen und somit zwangsweise Risiken eingehen. Wirtschaften zwingt uns zum ständigen Abwägen zwischen Chancen und Bedrohungen.

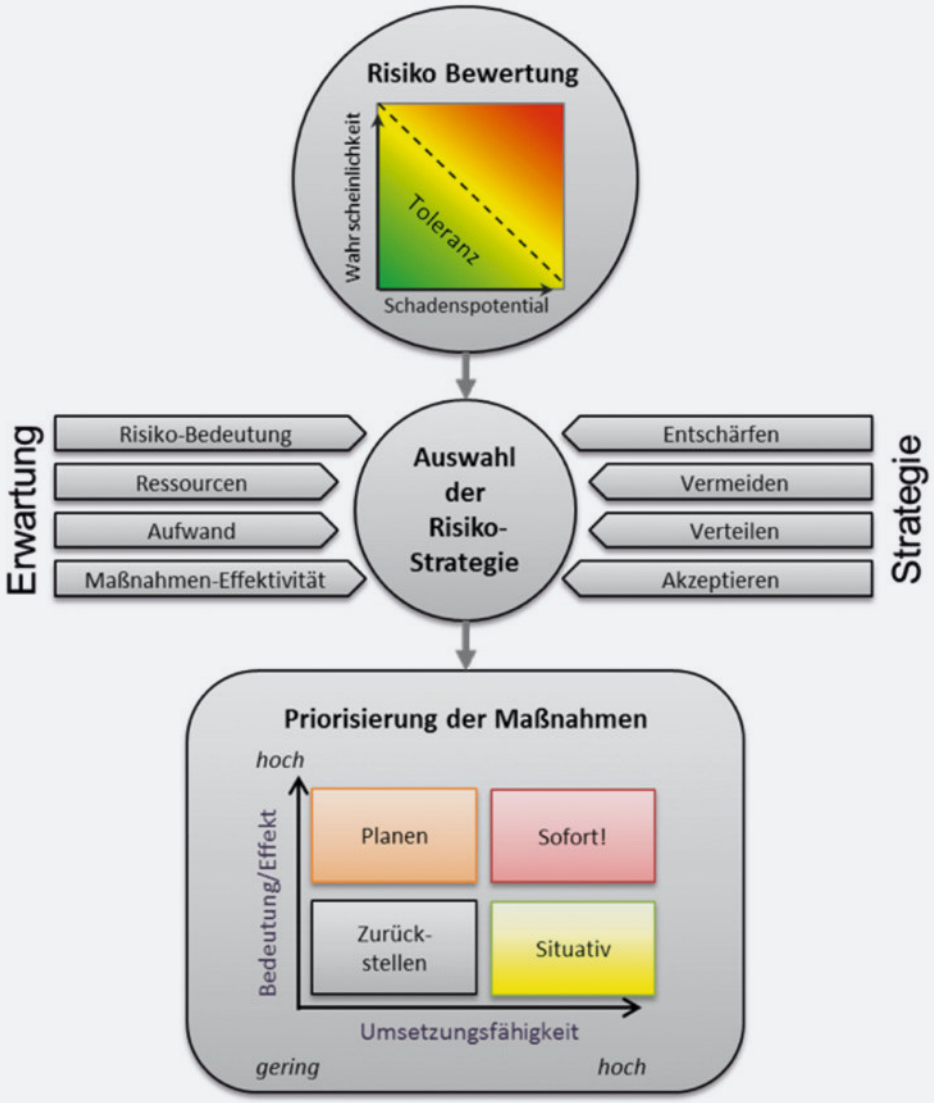
Risiko-Management bedeutet daher auch nicht, alle Risiken auszuschließen oder „zu minimieren“. Vielmehr geht es im Risiko-Management darum, die Risiken transparent zu machen, um Risiko-bewusste Entscheidungen in Bezug auf Chancen treffen zu können. Im Risiko-Management wird in diesem Zusammenhang auch gerne vom Risiko-Appetit eines Unternehmens gesprochen.

Die Einschätzung zu einer Bedrohung hängt maßgeblich von den getroffenen Maßnahmen gegenüber der Bedrohung als auch vom erwarteten Nutzen ab. Diese Einschätzung kann natürlich nur von der Kunden-/Nutzerseite getroffen werden. Um eine belastbare Abschätzung der eigenen Risiko-Position treffen zu können, ist allerdings der transparente Umgang mit Bedrohungen und den gegen sie getroffenen Maßnahmen eine Grundvoraussetzung.
Vor diesem Hintergrund ist das Management von Risiken sowohl auf der Serviceanbieter-Seite als auch auf der Nutzerseite wichtig.

Zum Umgang mit Risiken gibt es verschiedene etablierte ISO Normen, die zum Teil eine Spezialisierung bezüglich der IT aufweisen:

31000 Risk management – Principles and Guidelines on Implementation
31010 Risk management – Risk assessment techniques
27005 Information security – Risk management

Das grundsätzliche Vorgehen einer Risiko-Bewertung lässt sich wie folgt darstellen:



Der Risiko-Bewertungs- und Priorisierungsprozess

Gemeinsam durch die ISACA und die RMA (Risk Management Association) wurde im Juni 2014 ein „Leitfaden ISO 31000 in der IT – mit Vergleich zu anderen Standards“ veröffentlicht, der sich neben der Vermittlung gemeinsamer Grundlagen auch detaillierter mit den Unterschieden und Besonderheiten der benannten Normen, aber auch Cobit, den Risiko-Ausführungen im Rahmen des BSI Grundschutz-Standards 100-3 sowie verschiedenen Risiko-Bewertungsmethoden befasst.

Compliance

Compliance bezeichnet die Einhaltung von Gesetzen, Verordnungen, verbindlichen Normen und Regeln sowie Selbstverpflichtungen in Form von eigenen Richtlinien oder mit Dritten geschlossenen Verträgen. Das regulative Umfeld für IT im Allgemeinen und für Cloud Computing im Speziellen ist vielfältig und komplex. Zudem potenzieren die globalen Lieferketten die berührten Gesetzes- und Normenlandschaften, da die Regeln der verschiedenen „Teilnehmer-Länder“ an der Leistungsbereitstellung oder Nutzung zu berücksichtigen sind. Nachfolgend werden die wichtigsten Compliance-Bereiche thematisiert, die für Cloud-Anwendungen regelmäßig bedeutsam sind. Diese können jedoch von Branche zu Branche und von Unternehmen zu Unternehmen verschiedene Ergänzungen erforderlich machen.

Auditierung/Zertifizierung

Compliance geht einher mit dem Nachweis und der Prüfbarkeit des korrekten oder angemessenen Verhaltens. Die entsprechende Prüfung und Dokumentation durch einen unabhängigen Prüfer wird als Audit bezeichnet. Solche Prüfungen können sowohl gesetzlich vorgeschrieben sein, wie zum Beispiel in Form der Jahresabschlussprüfung von Aktiengesellschaften. Audits können aber auch durch Kunden durchgeführt werden oder freiwillig, um die Vertrauenswürdigkeit als Wettbewerbsfaktur zu nutzen, um sich auf externe Audits im Sinne einer Vorprüfung vorzubereiten oder auch als Bestandteil des eigenen Internen Kontrollsystems. Eine darauf spezialisierte Abteilung ist typischerweise die Interne Revision.

Durch die Berufsverbände der Prüfer/Auditoren werden häufig Prüfungsleitfäden herausgegeben. Sie sind meistens für die im Verband organisierten Prüfer richtungsweisend oder bindend. Sofern man beabsichtigt einen positiven Audit zu erlangen, ist es daher ratsam, die Prüfungsschwerpunkte und Erwartungen solcher Prüfungsleitfäden zu kennen und die eigene Organisation daran zu orientieren. Zumindest sollte man gute Argumente dafür parat haben, warum man ggf. von den Empfehlungen abweicht.

Oftmals bilden diese Prüfungsstandards sogar für offizielle Stellen und die Rechtsprechung einen wichtigen Bezugsrahmen im Sinne der üblicherweise zu erwartenden Vorgehensweisen. So werden bspw. durch den Fachausschuss für Informationstechnologie (FAIT) Stellungnahmen, Vorgehens- und Prüfungsempfehlungen herausgegeben, die rechtliche Aspekte aber

auch „übliche Praxis-Prinzipien“ konkretisieren und die von den Steuerbehörden und Finanzgerichtsbarkeit als Praxisstandard in der Regel auch anerkannt werden. Die IDW Prüfungsstandards (IDW PS) spielen in Deutschland eine wichtige Rolle, da sie Grundlage der meisten Jahresabschlussprüfungen sind.

Für die eigene Interessen-Sicherung ist die Auditierung und Zertifizierung durch unabhängige Zertifizierungsstellen ein durchaus übliches Verfahren, um die Prüfungsaufwende für alle Beteiligten gering zu halten. Allerdings bleibt die letztendliche Prüfungsverantwortung beim Auftraggeber. Leider kommt es immer wieder vor, dass Zertifikate präsentiert werden, die nicht geeignet sind, den Prüfungsgegenstand abzudecken. Zudem werden sogar werbewirksame Zertifikate kreiert, deren Prüfungsaussagen jedoch bei genauerem hinsehen wertlos sind. Bei der Beurteilung der angebotenen Zertifikate und Zertifizierer ist daher Sorgfalt geboten.

Compliance Management

Die Verletzung von Gesetzen und Regeln kann sowohl für das Unternehmen als auch für das Management höchst unangenehme Folgen haben. Schadensersatzansprüche und Strafzahlungen in Milliardenhöhe haben schon manches Unternehmen empfindlich getroffen oder gar in die Insolvenz getrieben. Auch Manager sehen sich mit Strafzahlungen, Haftungsansprüchen ihrer (Ex-) Arbeitgeber oder Haftstrafen konfrontiert. Eine sinnvolle Strategie diese Risiken zu reduzieren, ist die Einführung eines Compliance Management-Systems. Die systematische Identifikation und Bewertung relevanter Regularien, sowie die Etablierung und Kontrolle adäquater Compliance-Maßnahmen reduziert die Gefahr, wichtige Gesetze oder Regeln zu missachten. Zudem reduziert sich das Risiko für das Management, da ein möglicher Vorwurf der Fahrlässigkeit oder eines Organisationsverschuldens deutlich schwieriger zu begründen ist. Nicht zuletzt wird bei der Verhängung der Strafen regelmäßig berücksichtigt, in welchem Maße das Unternehmen oder Manager bemüht gewesen sind, die Missachtung zu vermeiden.

Zentrale Standards für Compliance Management Systeme sind die ISO 19600 für die Ausgestaltung eines Compliance Management Systems sowie die in Deutschland veröffentlichte IDW PS980[21] als Prüfungsnorm der Wirtschaftsprüfer.

Urheberrecht

Die Weitergabe bzw. Vervielfältigung von urheberrechtlich geschützten Inhalten, wie z. B. Nachrichten-Auszügen, Veröffentlichungen und auch Software unterliegen dem Urheberrecht. Die Nutzung fremder Software aus der Cloud ist somit Standardfall des SaaS. SaaS Anbieter benötigen in jedem Fall entsprechende Nutzungsrechte für die Vervielfältigung in der Cloud.

[21] IDW = Institut der Wirtschaftprüfer

Hinsichtlich der Nutzungsseite wird zwar in der juristischen Diskussion tendenziell die Nutzung über die Cloud nicht als Vervielfältigung angesehen. Aufgrund abweichender Meinungen und dem Fehlen einschlägiger Präzedenzfälle bleibt jedoch ein Risiko für den Nutzer. Deshalb sollten entsprechende Nutzungsrechte vertraglich abgesichert bzw. vereinbart sein.

Da Nutzungsrechte häufig länderspezifisch verhandelt werden, stellt die Bereitstellung von Inhalten in potenziell die Landesgrenzen überschreitenden Services ein rechtliches Problem dar. (Vielleicht wurden Ihnen in Youtube auch schon mal die Anzeige eines Musik-Videos unter Hinweis auf fehlende Landesrechte verweigert?)

Die EU plant daher im Rahmen ihrer Digitalen Agenda die EU-weite Harmonisierung der Urheberrechte, um der gewachsenen Mobilität der Bürger und ihrem Wunsch, ihre (rechtmäßig erworbenen) Inhalte aus jedem Land der EU abrufen zu können, gerecht zu werden.

Datenschutz

Datenschutz aus Compliance-Sicht betrachtet rechtliche Vorgaben für besonders schützenswerte Daten. Diese ergeben sich für die meisten Datenverarbeiter vor allem aus dem Schutz personenbezogener Daten. Hier sind vor allem auf nationaler Ebene das Bundesdatenschutzgesetz (BDSG) zu berücksichtigen sowie für besonders schützenswerte Daten der §203 des Strafgesetzbuches (StGB), der die Geheimhaltung besonders sensibler Daten im Rahmen der Ausführung bestimmter Berufe regelt, bzw. deren Weitergabe unter Strafe stellt. Dies betrifft z. B. medizinische Berufsgruppen, Versicherungen, Anwälte, Steuerberater, Sozialberufe, aber auch Amtsträger oder Wissenschaftler, die mit personenbezogenen Studiendaten arbeiten.

Open Source

Open Source Software erfreut sich großer Beliebtheit in vielen Teilen der Entwicklerschaft. Allerdings ist die Nutzung im Rahmen von Cloud-Lösungen nicht immer unproblematisch.

- Für Open Source Software werden zwar die Nutzungsrechte in der Regel unentgeltlich zur Verfügung gestellt. Daran knüpft sich allerdings auch häufig die Bedingung, dass das entstehende Gesamtwerk ebenfalls nur unentgeltlich weitergegeben werden darf (sogenannte Copy-Left-Lizenzen). Es wird in diesem Zusammenhang auch vom viralen Effekt der Copy-Left-Lizenzen gesprochen: Die Nutzung solcher Copy-Left-Lizenzen „infiziert“ darauf aufbauende Lösungen. Einige Hersteller von Open-Source Software haben bereits darauf reagiert und veröffentlichen ihre Angebote unter Lizenzbedingungen, bei denen durch entsprechende Klauseln sichergestellt ist, dass eine Weitergabe im Rahmen von Cloud auch kommerziell zulässig ist[22].
- Viele Lizenzbedingungen sind international und wurden vor dem Hintergrund des jeweiligen Landesrechts (häufig USA oder Skandinavien) erstellt. In anderen Ländern müssen diese Normen und ihre Begriffe ausgelegt werden, was zu Interpretations-Risiken führen kann. (Ist beispielsweise SaaS eine Weitergabe oder nur eine Nutzung?)

---

[22] z. B. die aktuelle GNU Affero General Public License / http://www.gnu.org/licenses/agpl-3.0

- Es gibt eine Vielzahl unterschiedlicher Nutzungsbedingungen. Basiert die eigene Software auf vielen verschiedenen Open-Source-Schnipseln, die ebenfalls auf unterschiedlichen Nutzungsbedingen gründen, erhält man ein nur schwer aufzulösendes Potpourri an Weitergabe-Bedingungen für das spätere Gesamtwerk. Hieraus eigene Weitergabebedingungen zu formulieren, kann schwer oder gar aufgrund von Widersprüchen unmöglich sein.

Es isst daher ratsam, bereits bei der Auswahl von OpenSource-Software aufzupassen, ob diese auch rechtlich einwandfrei integriert werden kann.

Finanzsysteme

Abrechnungssysteme sind häufig Bestandteil von Cloud-Systemen. Entsprechend sind die hierfür einschlägigen Gesetze und Standards zu berücksichtigen. Neben Handels- und Steuergesetzen sind dies insbesondere die GOB[23]/GoBD[24], sowie die ergänzenden Stellungnahmen des IDW[25] insbesondere des FAIT[26] bzw. im internationalen Kontext die IFRS[27] sowie die SOC bzw. SOC-1 in den USA. SOC-1 richtet sich auf die internen Kontrollen im Rahmen der Finanzberichterstattung (ICoFR). Hierfür gibt es präzisierende Prüfungsgrundlagen in Form des Standards SSAE 16 (ehem. SAS 70; vgl. auch Abschnitt Corporate Governance/Interne Kontrollsysteme!)

Payment

Services für die Zahlungsabwicklung sind lukrativ und versprechen Kundenbindung. Sie sind aber auch anspruchsvoll bezüglich der Sicherheitsanforderungen.

Große Finanzorganisationen und Kreditkartenanbieter versuchen faktische Zahlungsstandards zu setzen (z. B. Paypal, Giropay). Doch es gibt immer wieder neue Anbieter, die beispielsweise versuchen, Zahlungen über mobile Geräte und deren neue technische Möglichkeiten (z. B. NFC[28]) zu etablieren (z. B. KES, Pay Direct, ApplePay).

Ein etablierter Sicherheitsstandard ist der Payment Card Industry Data Security Standard, kurz PCI-DSS, der von allen wichtigen Kreditkartenorganisationen unterstützt wird.

Die gegenüber Mitgliedern teils sogar mit Sanktionen belegten Standards betreffen vor allem technische und organisatorische Sicherheitsstandards sowie Sicherheitsaudits, die abhängig vom Volumen und anderen Rahmenbedingungen von Selbstauskünften bis hin zu regelmäßigen externen Prüfungen reichen.

---

[23] Grundsätze ordnungsmäßiger Buchführung
[24] Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
[25] Institut der Wirtschaftsprüfer
[26] Fachausschuss für Informationstechnologie
[27] International Financial Reporting Standards
[28] Near Field Communication

Export

Moderne Software-Entwicklung setzt vielfach auf Komponenten von Drittanbietern auf. In vielen Ländern gibt es Export-Gesetzte, die eine Ausfuhr von verschiedenen Gütern, Technologien und Wissen in bestimmte Embargo-Länder streng reglementieren oder sogar ausschließen. Insbesondere in der USA, als Mutterland vieler Internettechnologien, gibt es teils harsche Export-Einschränkungen. Schon die Weitergabe von Informationen an Staatsbürger bestimmter Länder kann die Verletzung von Exportgesetzen zur Folge haben. Bei internationalen Geschäften sollte also genau darauf geachtet werde, welchen Einschränkungen eingesetzte Technologen und Lizenzen unterworfen sind und in welche Länder man bestimmte technologische Güter und Informationen weitergibt.

Verträge

Verträge sind für Wirtschaftsunternehmen die Grundlage jeder Leistungsbeziehung. Sie entscheiden sowohl über die gegenseitigen Verpflichtungen als auch über etwaige Ansprüche (Haftung) im Falle der Nichteinhaltung. Verträge spiegeln das Spannungsfeld zwischen den Vertragsparteien wieder, eine möglichst günstige Position zu erlangen. Auch wenn in Deutschland in hohem Maße vertragliche Gestaltungsmöglichkeiten bestehen, sind nicht alle Vertragsformulierungen auch rechtlich zulässig und am Ende auch wirksam. Gerade AGB können bestimmte Haftungen nicht einfach ausschließen, jedoch durch geschickte vertragliche Konstruktionen einschränken. Entsprechend sind Verträge sorgfältig zu erstellen und Vertragsvorschläge der Gegenseite kritisch zu prüfen. Hierzu ist juristischer Sachverstand erforderlich.

Verbände bieten teilweise Mustersammlungen oder Checklisten an. Der BITKOM als Vertretungsverband der ITK-Industrie hat sich sehr umfassend mit der Vertragsseite auseinandergesetzt. Unter der Bezeichnung Cloud Computing – Was Entscheider wissen müssen stellt der Bitkom eine gute Beschreibung wichtiger Vertragsbestandteile Interessierten zur Verfügung. Die Initiative Trusted Cloud des BMWI hat zudem eine gute Thematisierung vertragsrechtlicher Problemstellungen unter dem Titel Leitfaden – Vertragsgestaltung beim Cloud Computing herausgegeben.

Rechtsberatung darf allerdings in Deutschland nur durch ausgebildete Rechtsanwälte erfolgen. Auf IT-Recht spezialisierte Kanzleien bieten ebenfalls Musterverträge an und helfen bei der Prüfung von Anbieterverträgen oder unterstützen ggf. bei der Ausarbeitung von speziell erforderlichen Inhalten. Die Vergabe an einen Anwalt bietet zudem den Vorteil, dass im Falle einer Falschberatung, der Anwalt Schadensersatz-pflichtig werden kann. In der Regel sind Anwälte gegen derlei Unannehmlichkeiten versichert.

Nicht immer lassen sich die Verträge nachverhandeln. Mitunter bleibt nur die Lösung, sich einen anderen Anbieter zu suchen, der an einem fairen Interessensausgleich interessiert ist.

Vertragliche Besonderheiten in der Cloud
Nachfolgende Aspekte sollten beim Eingehen eines Cloud-Vertrages unbedingt beachtet beziehungsweise sorgfältig geprüft werden:

Auftragsdatenverarbeitung
Die wenigsten Cloud Services laufen anonym ab. Daher sind fast immer personenbezogene Daten im Spiel. „Personenbezug" bedeutet, dass bereits ein Rückschluss auf die Person ausreicht, um personenbezogene Daten zu verarbeiten. Also auch IDs, oder die Adresse können bereits ausreichen, um personenbezogene Daten zu verarbeiten.

Sofern keine explizite Einwilligung der Betroffen zu einer Weitergabe der Daten an Dritte vorliegt, räumt das Bundesdatenschutzgesetz nur wenig Spielraum für die Einbindung Dritter in den Service-Prozess ein. „Betroffene" sind übrigens diejenigen, deren Daten verarbeitet werden. Und Dritte sind alle Partner und Dienstleister, die potenziellen Zugriff auf die Daten, zum Beispiel im Rahmen von Wartungsarbeiten, haben könnten. Ein üblicher Weg, dem Datenschutz dennoch gerecht zu werden, ist der Abschluss eines Auftragsdatenverarbeitungsvertrages. Dieser stellt im Interesse des Auftraggebers – also dem Kunden des Portals – vor allem Transparenz über das Verfahren und eine etwaige Weitergabe von Daten sicher. Außerdem räumt er bestimmte Vorgabe- und Kontrollrechte ein, die ein datenschutzkonformes Verhalten gegenüber dem Auftragnehmer vertraglich sicherstellen.

Neben dem eigentlichen Auftragsdatenverarbeitungsvertrag sind die Verfahrensbeschreibung sowie die sogenannten Technisch-Organisatorischen Maßnahmen, kurz TOM, zwei wichtige Bestandteile des Auftragsdatenverarbeitungsvertrages. Deren Inhalte werden durch das Datenschutzgesetz strukturell sehr detailliert vorgegeben. Die Verfahrensbeschreibung macht in Grundzügen transparent, welche personenbezogenen Daten, wie und durch wen verarbeitet werden. Die Technisch-Organisatorischen-Maßnahmen listen für wesentliche im Datenschutzgesetz thematisierte Verfahrensrisiken die konkreten technischen Maßnahmen auf, die ein angemessenes Sicherheitsniveau garantieren sollen. Als Zertifizierungen für die TOMs werden häufig Zertifizierungen nach ISO 27001 oder BSI Grundschutz eingesetzt. (Vgl. auch Abschnitt Auditierung/Zertifizierung!)

Export-Klausel-Kennzeichnung
Wie im Abschnitt „Export“ thematisiert, kann es bei Cloud-Nutzung regelmäßig zu Exportsituationen kommen. Vertraglich sollte daher die Nutzung in den angestrebten Nutzungsländern abgesichert werden.

Gewährleistung
Kunden wollen möglichst eine unbegrenzte Haftung des Anbieters, wohingegen der Anbieter möglichst keine Garantien gewähren möchte. Hierbei handelt es sich um einen klassischen Interessenskonflikt.

Noch nicht sehr verbreitet, jedoch ein durchaus bedenkenswerter Baustein der Risiko-Begegnungs-Strategie sind Versicherungen gegen sogenannte Cyberrisiken. Mit Ihnen lassen sich Schadensfälle zwar nicht vermeiden, Ihre Wirkungen aber abmildern. Allerdings sollten sie nicht dazu führen, keine eigenen Sicherheitsbemühungen anzustrengen!

Exit
Verträge sollten von Beginn an sicherstellen, wie der Nutzer am Ende eines Services an seine Daten herankommt. Entsprechende Klauseln müssen den konkreten Anforderungen in Hinblick auf Rechtsnotwendigkeiten (z. B. Aufbewahrungsvorgaben, Eigentumsrechte an den Daten), Kompetenzen (Kann ich mit dem Zurückgelieferten etwas anfangen?), Ressourcen (Erfolgt die Übergabe zeitnah?) und besondere Situationen (z. B. Insolvenz) gerecht werden.

Solche Überlegungen und Lösungs-Strategien sollten vorab geklärt werden, damit sie in den Verträgen Berücksichtigung finden können.

8. MARKTPLÄTZE/APP STORES/ SERVICE INTEGRATION

Erwartungen

Marktplätze richten sich typischerweise an eine bestimmte Klientel. Dies gilt für öffentliche Online-Marktplätze ebenso wie für Konzern-eigene App Stores oder Ressourcen-orientierte Angebote, die eher einer Börse gleichen.

Sieht man einmal von bunten Basaren und Flohmärkten ab, deren „Verführung“ im Bummeln und mußevollen Entdecken liegt, sind die meisten Geschäftsmarktplätze wohl eher von der Erwartung eines effizienten Einkaufs- und Nutzungs-„Erlebnisses“ geprägt. Bei Börsen-artigen Handelsplätzen für IT ist ein hoher Automatisierungs- und Integrations- Grad für die Abnehmerseite eine zwingende Voraussetzung, insbesondere weil als wichtige Zielgruppe das Internet of Everything bzw. Industrie 4.0 gesehen werden.

Consumer

De facto Standards im Consumer-Bereich setzen hier bislang vor allem die allseits bekannten Shops, wie Amazon oder die großen App Stores von Apple, Google und Microsoft. Allgemein bekannte Elemente wie beispielsweise Suchfunktionen, Rezensionen oder der Einkaufswagen als Symbol für die ausgewählten Waren finden sich vielfältig wieder und tragen zur Orientierung und Akzeptanz bei den Nutzern bei. Die zusammengefasste Abrechnung von möglicherweise verschiedenen Lieferanten gehört ebenso zum erwarteten de facto Standard in Shop-Umgebungen.

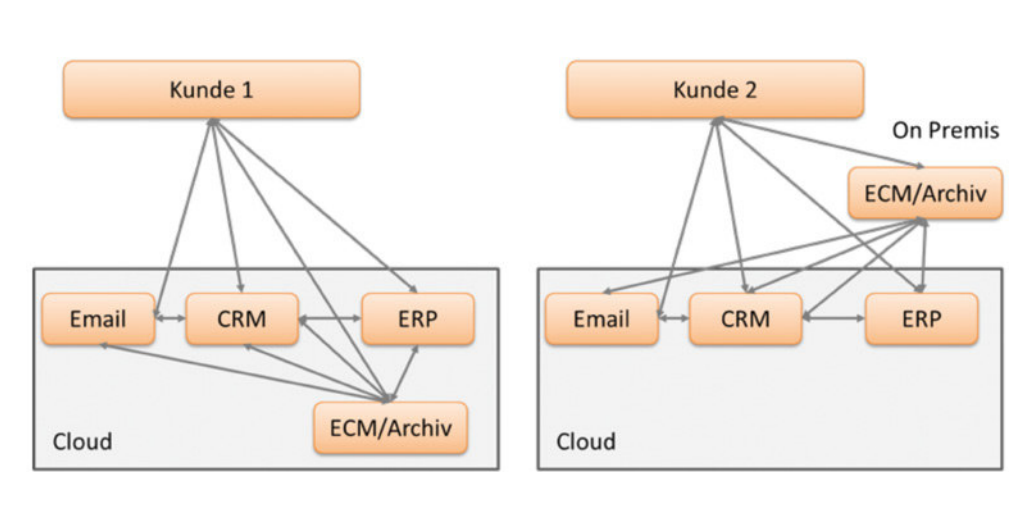
Infrastruktur-Handelsplätze

Handelsplätze für Speicher und Rechenkapazitäten unterschiedlicher Hersteller sind noch ein junges Unterfangen. Die Deutsche Börse befand sich mit ihrem Spin-Off „Deutsche Börse Cloud Exchange“ seit Ende Mai 2015 auf dem Markt, hat den Betrieb aber im Januar 2016 bereits wieder eingestellt.

Bemerkenswert ist die Intercloud-Initiative, mit dem Ziel eine verteilte Cloud- basierende Netzwerk- und Sicherheitsarchitektur zu entwickeln. Neben den Standardanforderungen, wie Skalierbarkeit und einfache Integrationsmöglichkeiten, soll sie vor allem in der Lage sein, umfassend Compliance mit lokalen Datenschutzregeln abzubilden. Sie setzt auf OpenStack auf und wird von einer Reihe namhafter Firmen unterstützt. Besonders intensiv engagiert sich Cisco. Die Deutsche Telekom als nationales Cloud-Schwergewicht gehört ebenfalls zu den aktiven Unterstützern. Es fehlt jedoch derzeit noch an praktischen Erfahrungsberichten.

Integrierte Services

Waren an einen Besteller zu liefern, ist eine recht einfache Transaktion. Schwieriger wird es, wenn Services in unterschiedlicher Intensität von unterschiedlichen Stellen einer Organisation genutzt werden sollen und mehrere Services möglicherweise sogar miteinander agieren können – wenn also Services in einen Meta-Service integriert werden sollen.



Beispiel: Eine eingehende Email mit einer Bestellung (Email-System) soll beispielsweise im Kundenmanagement (CRM) bekannt gemacht werden und sowohl eine Warenlieferung als auch die Rechnungsstellung veranlassen (ERP). Die dabei entstehenden Dokumente sollen schließlich rechtskonform archiviert werden (ECM). Dabei ist die Abgrenzung für den einzelnen Mandanten sicherzustellen.

Die Abrechnungsseite ist dabei noch eine relativ überschaubare Herausforderung, da es „nur“ um ein abgestimmtes Messen der Inanspruchnahme von Leistungen geht, also um die Erfassung von Volumina, Transaktionen oder angemeldeter Benutzer und deren Zuweisung an mit ihnen in Zusammenhang stehenden Abrechnungsempfängern. Es geht also darum die Abrechnungsdaten zu vereinheitlichen und anhand vereinbarter Regeln in einer übergeordneten Anwendung zusammenzuführen.

Viele namhafte Anbieter haben versucht, verschiedene Cloud-Angebote in einem gemeinsamen Portal anzubieten. Kommerziell bleiben diese Angebote jedoch bislang hinter den (meist hochgesteckten) Erwartungen zurück. Nur wenige Anbieter scheinen den notwendigen „Langen

Atem“ und ausreichende Attraktivität für Anbieter und Nachfrager zu haben, wie z. B. App Direct oder die Deutsche Telekom. Offenbar gelingt es derzeit noch nicht, ausreichend Vorteile für die Nutzer zu generieren.

Solange solche Portale nur als neuer Vertriebsweg angesehen werden und die verschiedenen Services im Kern nur unabhängig voneinander genutzt werden können, steht zu befürchten, dass sich daran auch nichts signifikant ändert. Geschäftsprozesse halten sich nicht an Systemgrenzen und müssen über diese hinaus verarbeitet werden.

Solche Integrationen stellen jedoch eine weitaus größere Herausforderung dar: Der Datenaustausch zwischen Services erfordert verlässliche Schnittstellen für die Daten-Migration und Synchronisierung unterschiedlichster Services und für die Meta-System-weite Steuerung (vgl. auch Abschnitt „Prozessintegrationsstandards“!). Zudem bestimmt das schwächste Glied die Verlässlichkeit der Service Level. Es fordert von den verschiedenen Service-Anbietern die Bereitschaft und Fähigkeit, vorgegebene Service-Level einzuhalten.

Im traditionellen On-Premise-Geschäft besteht zwar die Möglichkeit, sich einen Anbieter mit einem möglichst umfassenden Funktionsportfolio zu suchen. Alternative Komponenten sind in diesem Modell jedoch meist nur am Rande zu finden und hängen am Wohlwollen und der Unterstützung des Kernanbieters. Solche partiellen Monopol-Positionen erlauben den Herstellern, attraktive Margen zu realisieren – zulasten der Kundenbudgets. Diese Abhängigkeit zugunsten eines modularen Service-Marktplatzes aufzulösen, gehört zu den attraktivsten, aber auch herausforderndsten Chancen des Cloud-Computings.

Einen frühen Ansatz gab es 2009. Das von SAP vorgestellte Konzept einer offenen Service-Beschreibung UDSL (Unified Service Description Language), konnte sich in der Praxis bislang jedoch nicht etablieren.

Erfolgversprechende Initiativen sind tendenziell seitens großer Infrastrukturanbieter zu erwarten. IBM Cast Iron und Elastic.io (seit neuestem in Kooperation mit der Deutschen Telekom) sind aktuell bemüht, dieses Segment zu besetzen. Auch von der Anbieterseite kooperativ getriebene Ansätze, wie die German Businesscloud[29] mit dem Cloud WorkPlace, haben das Potenzial, Marktsegmente erfolgreich zu adressieren. Ob sie es schaffen, geschäftstaugliche Service-Integrationen am Markt zu etablieren und ob sich noch weitere Kandidaten aus der Marktplatz-Szene dazugesellen, wird sich zeigen.

[29] www.germanbusinesscloud.de

9. AUSBLICK

Gesetze

EU-Digital-Strategie2015
In der Digital Agenda umreißt die EU-Kommission, welche Gesetzesvorschläge sie in den kommenden Jahren vorlegen möchte, um einen digitalen Binnenmarkt zu schaffen.

Die im Mai 2015 veröffentlichten Empfehlungen haben eine große Chance, in verschiedenen Gesetzen Realität zu werden. Insbesondere für die Anbieterseite empfiehlt es sich, die rechtliche Entwicklung in den skizzierten Bereichen im Auge zu behalten.

Die Bedeutung von Standards ist in der dritten Säule explizit zu erkennen.

Nachfolgend in Auszügen, die für Cloud Computing bedeutsamsten Empfehlungen und Vorhaben:

Zu den 3 Säulen der Strategie für einen digitalen Binnenmarkt sind 16 zentrale Maßnahmen vorgesehen, die die Kommission **bis Ende 2016** umsetzen wird:

Säule I: Besserer Zugang für Verbraucher und Unternehmen zu digitalen Waren und Dienstleistungen in ganz Europa

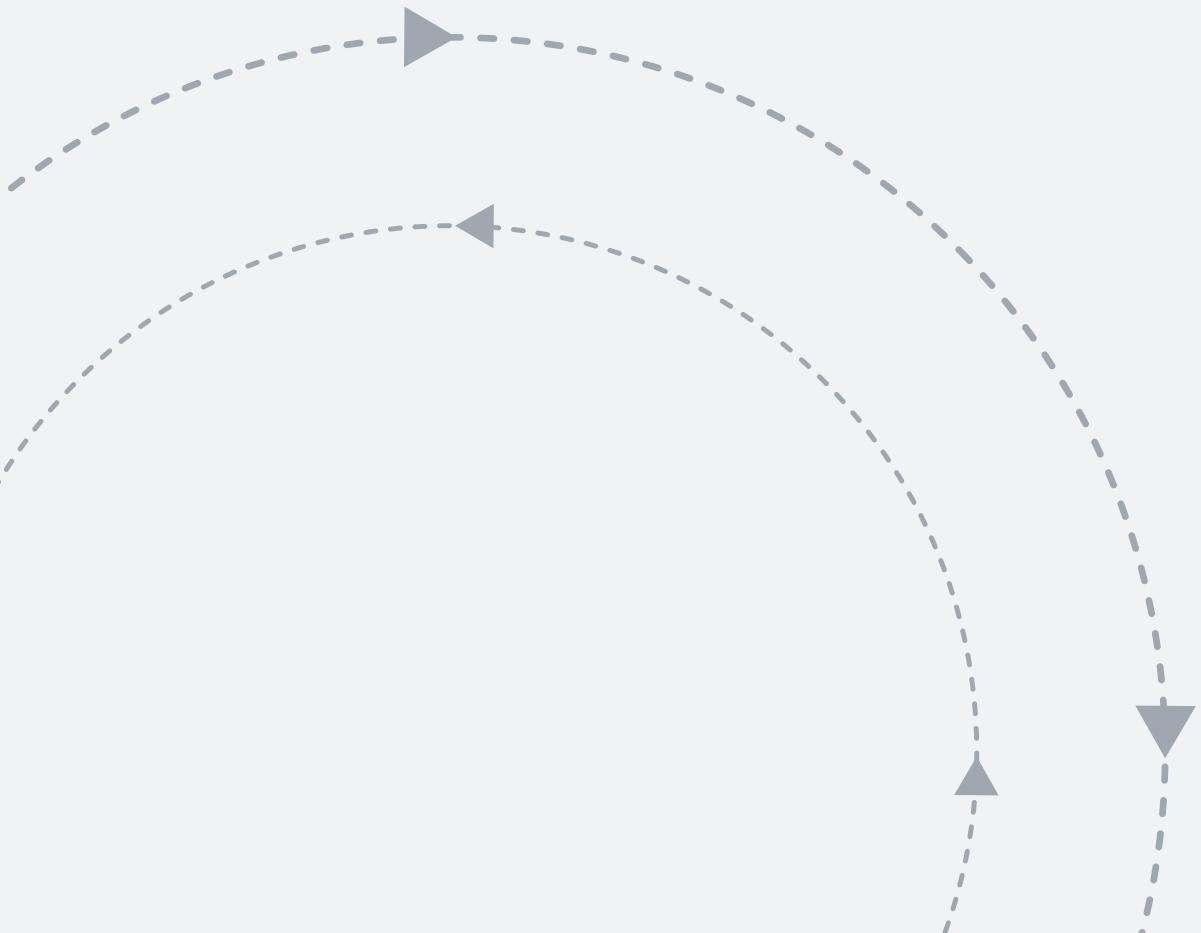
1. Regeln zur Erleichterung des grenzüberschreitenden elektronischen Handels. Dies umfasst harmonisierte EU-Vorschriften über vertragliche Aspekte sowie den Verbraucherschutz bei Online-Käufen. …
2. Eine raschere und kohärentere Durchsetzung des Verbraucherrechts durch die Überarbeitung der Verordnung über die Zusammenarbeit im Verbraucherschutz.
6. Ein modernes, europäischeres Urheberrecht

Säule II: Schaffung der richtigen Bedingungen und gleicher Voraussetzungen für florierende digitale Netze und innovative Dienste

10. den Rechtsrahmen für audiovisuelle Medien zu überprüfen, … Hierbei wird die Rolle der einzelnen Marktteilnehmer (..) bei der Förderung europäischer Werke im Mittelpunkt stehen. Die Kommission wird auch untersuchen, wie die derzeit geltenden Bestimmungen (..) so gestaltet werden können, dass sie neuen Geschäftsmodellen für die Verbreitung von Inhalten gerecht werden.
11. die Rolle von Online-Plattformen (Suchmaschinen, soziale Netze, App-Stores usw.) auf dem Markt eingehend zu analysieren. Soweit dies nicht bereits im Wettbewerbsrecht geregelt wird, betrifft dies Themen wie die mangelnde Transparenz bei den Suchergebnissen und in der Preispolitik, die Nutzung der von Plattformen gesammelten Daten, die Beziehungen zwischen Plattformen und Anbietern und die Bevorzugung eigener Dienste zum Nachteil von Wettbewerbern. …
12. das Vertrauen und die Sicherheit bei digitalen Diensten insbesondere beim Umgang mit personenbezogenen Daten zu stärken. Auf der Grundlage der neuen EU-Datenschutzvorschriften, die bis Ende 2015 angenommen werden sollen, wird die Kommission eine Überprüfung der e-Datenschutz-Richtlinie einleiten.

Säule III: Bestmögliche Ausschöpfung des Wachstumspotenzials der digitalen Wirtschaft

14. …Initiative zum „freien Datenfluss“ …, um den freien Datenverkehr in der EU voranzubringen. Mitunter können sich neue Dienste aufgrund von Beschränkungen hinsichtlich des Standorts der Daten oder des Zugang zu den Daten nicht entfalten, obwohl solche Beschränkungen häufig gar nicht dem Schutz personenbezogener Daten dienen. Diese neue Initiative wird solche Beschränkungen beseitigen …. Die Kommission wird ferner eine europäische Cloud-Initiative vorstellen, in der es um die Zertifizierung von Cloud-Diensten, die Möglichkeit des Wechsels des Cloud-Diensteanbieters und um eine Forschungs-Cloud gehen wird.
15. Prioritäten für die Normung und Interoperabilität in Bereichen festzulegen, die für den digitalen Binnenmarkt eine zentrale Bedeutung haben, z. B. e-Gesundheit, Verkehrsplanung und Energie (intelligente Verbrauchsmessung).
16. … Durch einen neuen e-Government-Aktionsplan sollen außerdem …, die Kompatibilität unterschiedlicher nationaler Systeme sichergestellt und dafür gesorgt werden, dass Unternehmen und Bürger ihre Daten nur einmal an die öffentliche Verwaltung übermitteln müssen und Behörden nicht länger mehrfach dieselben Informationen abfragen, wenn ihnen diese Angaben bereits vorliegen. … Die Einführung der elektronischen Auftragsvergabe (e-Beschaffung) sowie interoperabler elektronischer Signaturen wird beschleunigt werden.



IT Sicherheitsgesetzt (für kritische Infrastrukturen)
Im Juni 2015 wurde das IT Sicherheitsgesetzt durch den Bundestag beschlossen. Es fordert von den Betreibern kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen.

Die Maßnahmen sind nicht im Detail vorgeben, sondern sollen sich an der konkreten Situation und am Stand der Technik orientieren. In der Begleitdokumentation gibt es bereits Hinweise auf ISO-Normen, so dass die Orientierung und gegebenenfalls Zertifizierung nach den einschlägigen ISO-Standards (insbesondere der ISO 27001) die Erfüllung der Anforderungen gut begründen dürfte.

Betroffene Unternehmen müssen die Mindestmaßnahmen zwei Jahre nach Erlass der Rechtsverordnung eingeführt haben und spätestens alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) dokumentieren. Zudem wird eine benannte Kontaktstelle erwartet, die jederzeit, also 24 Stunden an 7 Tagen, erreichbar ist. Außerdem müssen Ausfälle oder gravierende Einschränkungen gemeldet werden.

Betroffene Segmente sind Energie, Ernährung, Gesundheit, Informationstechnik, Telekommunikation, Transport und Verkehr, Wasser sowie Finanz- und Versicherungswesen, sofern ein Ausfall oder eine Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu einer Gefährdung der öffentlichen Sicherheit führen könnte. Damit ist der Kreis der unmittelbar Betroffenen deutlich eingeschränkt. Dennoch muss davon ausgegangen werden, dass von wichtigen Sub-Lieferanten mindestens in Teilen vergleichbare Sicherungs- und Vorsorge-Maßnahmen erwartet werden. Cloud-basierte Services stellen dabei keine Ausnahme dar.

Gesellschaft und Politik

Die Bedeutung von Informationen und der Technik, die diese verarbeitet, nimmt immer noch zu. Das World-Wide-Web wird seinem Namen zunehmend gerecht. Der Internet-Zugang verbreitet sich selbst in Entwicklungsländern rasant. In den Industrie-Nationen werden die Übertragungskapazitäten fieberhaft ausgebaut, um der explodierenden Nachfrage immer neuer Service-Angebote gerecht zu werden. Gleichzeitig sinken die Kosten für leistungsfähige Halbleiterelemente immer weiter. Bis vor wenigen Jahren ging es vor allem um Speicherkapazitäten und Prozessorleistung. Aktuelle Entwicklungen drehen sich vermehrt auch um Sensorik, Latenzzeiten[30] und die Integration auf kleinstem Raum, um die Verbindung zur Umwelt, dem Internet und seinen Cloud-basierten Services mobil und für Alltagsgegenstände wie Uhren, Lampen oder Kleidung zu ermöglichen. Es bedarf keiner prophetischen Gaben, einen anhaltenden Strom neuer Services und neuer digitaler Marktplätze vorauszusagen.

Vernetzung ist ein zentrales Thema und betrifft sowohl Devices, Services und Handelsplattformen unterschiedlicher Ebenen gleichermaßen. Dabei geht es um Effizienzgewinne, mehr Komfort, disruptive und neue Geschäftsmodelle – und natürlich um viel Geld.

---

[30] Verzögerung durch Datenübertragung bzw. Reaktionszeit

Vor allem wenn es gelingt, Services einem breiten Umfeld zugänglich zu machen, wächst die Attraktivität. Deshalb haben viele Unternehmen ein Interesse daran, Standards für Kunden, Partner und neue Möglichkeiten zu schaffen und diese aktiv zu unterstützen.

Wo auch immer es um viel Geld geht, steigt zudem die Versuchung von Missbrauch der neuen Möglichkeiten. Solchen Bedrohungen muss sich die Gesellschaft mithilfe gesetzlicher Rahmenbedingungen stellen. Dieser Wettlauf wird auch die nächsten Jahre begleiten. Mit den Initiativen wie der anstehenden EU-Datenschutznovelle oder den angekündigten Zertifizierungsvorschlägen der Trusted Cloud Initiative gehen fast immer auch Standards einher, die der Gesetzgeber vorgibt oder mit den Interessensverbänden der Gesellschaft gemeinsam abstimmt.

Die Entwicklung neuer Standards wird das Thema Cloud auch in Zukunft begleiten.

Unternehmen

Diese Entwicklungen im Blick zu behalten und für die eigenen Geschäftsaktivitäten zu beurteilen, ist eine Herausforderung. Überhaupt werden Cloud-Technologien unter den Vorzeichen des Internet of Everything und der Industrie 4.0 die meisten Unternehmen zunehmend beschäftigen. Deshalb wird es für Unternehmen vor allem darauf ankommen, die eigene Transformation in die digitale Welt zu meistern. Dies betrifft nicht alleine die IT und ihre sich ändernde Rolle vom „Produzenten“ von IT-Leistungen hin zu einem IT-Controller und Berater. Vielmehr geht es auch darum, die eigenen Geschäftsmodelle an die sich verändernde Umwelt anzupassen, vor disruptiven Markteinsteigern zu schützen beziehungsweise diesen zuvor zukommen. Sich selbst infrage zustellen, ist wohl die größte Herausforderung. Aber es gibt keine Alternative, wenn man unangenehme Überraschungen vermeiden möchte.

Deshalb beginnen immer mehr Unternehmen eine eigene „Digitale Agenda“ zu entwerfen und „Digitale Beiräte“ einzusetzen.[31] Es ist immer dann sinnvoll, unabhängige Komitees oder „Advisory-Boards“ zu installieren, wenn das „Beratungsfeld“ geeignet erscheint, dass Tagesgeschäft massiv zu verändern und Widerstände aus bestandsbewahrenden Verharrungsmotiven nicht auszuschließen sind. Neben visionären und innovationsfreudigen TOP-Managern des Unternehmens werden diese üblicherweise ergänzt mit erfahrenen Experten aus der Digitalwirtschaft. Sie bringen eine externe Perspektive mit. Ohne Linien-Bindung, Teams und eine oft jahrelange Betriebsprägung fällt es ihnen erfahrungsgemäß leichter, den Status Quo infrage zu stellen und ganz neue Ideen und Impulse einzubringen. Die typischen Aufgabenstellungen der Digitalen Beiräte sind die Erkennung von Chancen und Risiken digitaler Trends und ihrer Auswirkungen auf die eigenen Geschäftsmodelle, die Entwicklung „Digitaler-Transformations“-Strategien sowie die unterstützende Begleitung bei deren Umsetzung.

---

[31] Computerwoche v. 27.4.15, „Erfolgskritische Komponente in der digitalen Transformation“ http://www.computerwoche.de/a/erfolgskritische-komponente-in-der-digitalen-transformation,3097382

Spezielles Angebot zur CLOUD TRANSITION

Die Folker Scholz Unternehmensberatung (FSU) steht für ganzheitliche Beratung und ergebnisorientiertes Coaching, wenn IT die Geschäftsprozesse unterstützen soll. Mit dem CLOUD-TRANSITION-COACHING bietet sie spezielle Service-Pakte für den effektiven Weg in die Cloud Nutzung.

Mit der Cloud erfolgt zunehmend ein Teil der Leistungserbringung außerhalb der direkten Wahrnehmungs- und Einfluss-Sphäre. Die Anbieter und ihre Verfahren müssen gesteuert, kontrolliert und ihre Leistungen orchestriert werden. Dabei muss die Compliance sichergestellt werden. Nur so lassen sich ihre Vorteile effektiv nutzen, ohne dabei unwägbare Risiken einzugehen.

Von der IT wird plötzlich ein neues Profil erwartet. War ihre Aufgabe bislang die Produktion von IT-gestützten Leistungen, muss sie jetzt mehr Beratungs-, Evaluations-, Kontroll-, Auditierungs- und Managementaufgaben wahrnehmen. Diese umfassen Beratungskompetenz im Kontext der Compliance und neuer innovativer Geschäftsmodelle.

Cloud-Transition-Check

Wie vorbereitet sind Sie für die Cloud? Testen Sie Ihren Cloud-Bedarf und Ihre Cloud-Readiness! Über die CLOUD-TRANSITION-COACHING- Homepage können Ihren persönlichen Kurz-Test (10+10 Fragen) durchführen.

Cloud-Transition-Check Workshop

Wir bieten über das Cloud-Ecosystem ausgewählten Unternehmen kostenlos den individuellen Workshop Cloud-Transition-Check an. In diesem intensiven Beratungsgespräch analysieren wir ihre individuellen Chancen durch Cloud-Computing und die erforderlichen Voraussetzungen für eine effektiven und sicheren Weg in die Cloud.

CLOUD-TRANSITION-COACHING

Diese Metamorphose wird durch das CLOUD-TRANSITION-COACHING unterstützt und nachhaltig begleitet.

Erfahren Sie mehr über das Angebot unter:
Tel. +49-171-7441963
www.cloud-transition-coaching.de

IHR **EXPERTE**

Folker Scholz
Experte für die digitale Transformation
Mobil: +49-171-7441963
E-Mail: fscholz@folkerscholz.de

Ihr Experte für die digitale Transformation im Cloud-Ecosystem

Seit mehr als 25 Jahren unterstützt Folker Scholz Organisationen aus verschiedenen Branchen (u. a. Finanzdienstleistung, Industrie, IT und Verbände) im Umfeld Governance, Risk und Compliance als Berater und Coach. Zudem beschäftigt er sich seit einigen Jahren intensiv mit den Chancen und Risiken der digitalen Transformation im Allgemeinen und mit Cloud-Computing im Besonderen. Sein Angebot reicht von der klassischen projektbezogenen Beratung, über langfristiges begleitendes Coaching bis hin zur Arbeit als Digitaler Beirat. Seine Mitarbeit in verschiedenen Arbeitsgruppen und Verbänden erschließt ihm und seinen Mandanten die aktuellen Entwicklungen von Technologie, Compliance und Märkten. Neben dem Cloud Ecosystem ist er in folgenden Organisationen engagiert:

- Fachgruppe Cloud in der ISACA (Information Systems Audit and Control Association) CRISC (Certified in Risk and Information Systems Control)
- Bundesverband mittelständische Wirtschaft (BVMW)
- Institut für Betriebsberatung, Wirtschaftsförderung und -forschung (IBWF) – Zertifiziertes Mitglied im Beraternetzwerk
- Risk Management Association (RMA)
- Deutsches Netzwerk Wirtschaftsethik (DNWE)
- BAFA gelistet (Beratung ist KMU-förderfähig)
- Berater und Juror beim Businessplan Wettbewerb Berlin-Brandenburg

Zudem veröffentlicht er regelmäßig Kommentare und Fachaufsätze und referiert auf Kongressen und Fachveranstaltungen. Weitere Informationen finden Sie auf **www.cloud-transition-coaching.de** und **www.digitaler-beirat.de**

Kontakt: Mobil: +49-171-7441963, E-Mail: fscholz@folkerscholz.de