Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

EBERBACHER GESPRÄCH ZU »CLOUD COMPUTING«

09/2011

INHALT

LÖSUNGSANSÄTZE UND HANDLUNGSBEDARF

3.1 Sicherungsinstanz bei technischem Versagen

3.2 Einführung gemeinsamer Standards und Checklisten

3.3 Verständlichkeit

3

FAZIT

4

VORWORT

Angewandte Forschung zur IT-Sicherheit braucht den Dialog zwischen Wissenschaft und Wirtschaft, um anwendungsrelevante Antworten auf die grundsätzlichen Fragestellungen zu erhalten: Was sind die aktuellen Herausforderungen für IT-Sicherheit und Datenschutz in der Praxis? Was ist für die Zukunft zu erwarten? Was kann und soll Technik leisten, wo sind die Grenzen des Machbaren? Wo braucht es neue Ideen?

Die »Eberbacher Gespräche« des Fraunhofer SIT bieten ein Forum für diesen Dialog. Experten aus Wissenschaft und Wirtschaft treffen sich für jeweils einen Tag im Kloster Eberbach und erarbeiten für ein Thema gemeinsam Antworten auf diese Fragen. Im September 2011 ging es um »Sicherheit im Cloud Computing«. Teilnehmer waren

Dr. Harald Ahrens	SignCard GmbH
Dr. Thorsten Henkel	Fraunhofer SIT
Michael Herfert	Fraunhofer SIT
Dr. Michael Kaisser	AGT Group (R & D) GmbH
Thomas Koelzer	secunet Security Networks AG
Daniel Lentz	Deutsche Telekom AG
Prof. Dr. Ahmad-Reza Sadeghi	Fraunhofer SIT/TU Darmstadt
Dr. Jörg Spilker	DATEV eG
Prof. Dr. Michael Waidner	Fraunhofer SIT/TU Darmstadt
Dr. Steffo Weber	Oracle Deutschland GmbH

Die in diesem Papier dargestellten Ergebnisse werden von den Teilnehmern unterstützt, stellen aber nicht notwendigerweise die offizielle Sichtweise des jeweiligen Arbeitgebers dar.

MANAGEMENT SUMMARY

Cloud Computing wird als das IT-Trendthema der nächsten Jahre gesehen, Marktforscher sagen dem Konzept eine rosige Zukunft voraus. Der IT-Verband Bitkom errechnete für Cloud Computing in Deutschland im Jahr 2010 einen Umsatz von 1,2 Mrd Euro, 2012 soll sich diese Zahl bereits mehr als verdoppeln. Der Nutzen für Unternehmen und Behörden klingt verlockend: Mit Cloud Computing können IT-Strukturen wesentlich flexibler gestaltet und somit Kosten eingespart werden. Wer Hard- oder Software sowie Datenvolumen in die Wolke auslagert, kann Leistungsspitzen besser handhaben und Kosten für Beschaffung und Wartung einsparen.

Trotzdem hat sich das »Rechnen in der Wolke« noch nicht so flächendeckend durchgesetzt, wie man es angesichts dieser Vorteile erwarten könnte. Mit der Entscheidung, in die Cloud zu gehen, geben Nutzer einen Teil ihrer Unabhängigkeit an den Dienste-Anbieter ab und lagern wertvolle Unternehmensdaten aus. Dieser Schritt erfordert Vertrauen gegenüber dem Anbieter. Dieses Vertrauen kann der Anbieter durch eine größtmögliche Klarheit und Transparenz seiner Leistungen befördern Bei vielen Cloud-Diensten bleiben derzeit noch zahlreiche Fragen für potenzielle Nutzer unbeantwortet. Diese Unsicherheiten hindern Unternehmen und Behörden am Schritt in die Cloud.

Herausforderungen

Zum einen fehlt es an Standards, mit denen sich Cloud-Angebote gut vergleichen lassen: Vielen Cloud-Nutzern ist nicht klar, wie der Dienste-Anbieter im Detail mit ihren Daten umgeht. Daran schließt sich die Frage nach der IT-Sicherheit an. Wie geschützt sind ausgelagerte Daten in der Wolke wirklich? Hier fehlen Nachweise, die Nutzern eine vertrauliche Datenhaltung garantieren und gleichzeitig Schutz vor Angriffen von außen gewährleisten. Bei Cloud-Diensten kann es zudem zu Unklarheiten bei Rechtsfragen kommen, etwa in Bezug auf Datenschutz. Je nachdem, wo der Anbieter des Dienstes seinen Sitz hat, greifen unterschiedliche Rechtssysteme, was für den Nutzer nicht immer transparent ist.

Mitunter sind für den Cloud-Einstieg auch zusätzliche technische Aufwendungen nötig. So bleibt besonders für große Unternehmen die Frage, ob es sich tatsächlich lohnt, in die Cloud zu gehen. Ist der Schritt in die Cloud gemacht, bleibt die Frage, was geschieht, wenn der Cloud-Dienst nicht erreichbar ist. Hier fehlen Modelle für einen reibungslosen Cloud-Ausstieg oder -Wechsel.

Für all diese Probleme und Fragestellungen gibt es bislang noch zuwenig Pilotprojekte und Erfolgsmodelle, als dass sich allgemein gültige Regeln oder Handlungsanweisungen daraus ableiten ließen.

Lösungsansätze

Unternehmen und Behörden werden Cloud Computing nur nutzen, wenn die Angebote ausreichend Sicherheit und Handlungsfreiheit bieten. Dabei spielt zum einen der **Schutz der ausgelagerten Daten** eine entscheidende Rolle. Zum anderen muss der **gesicherte Zugriff** auf Daten und Prozesse gewährleistet sein. Um Cloud Computing vertrauenswürdiger und attraktiver für Nutzer zu machen, müssen Cloud-Anbieter für mehr **Klarheit und Verständlichkeit** der Angebote sorgen.

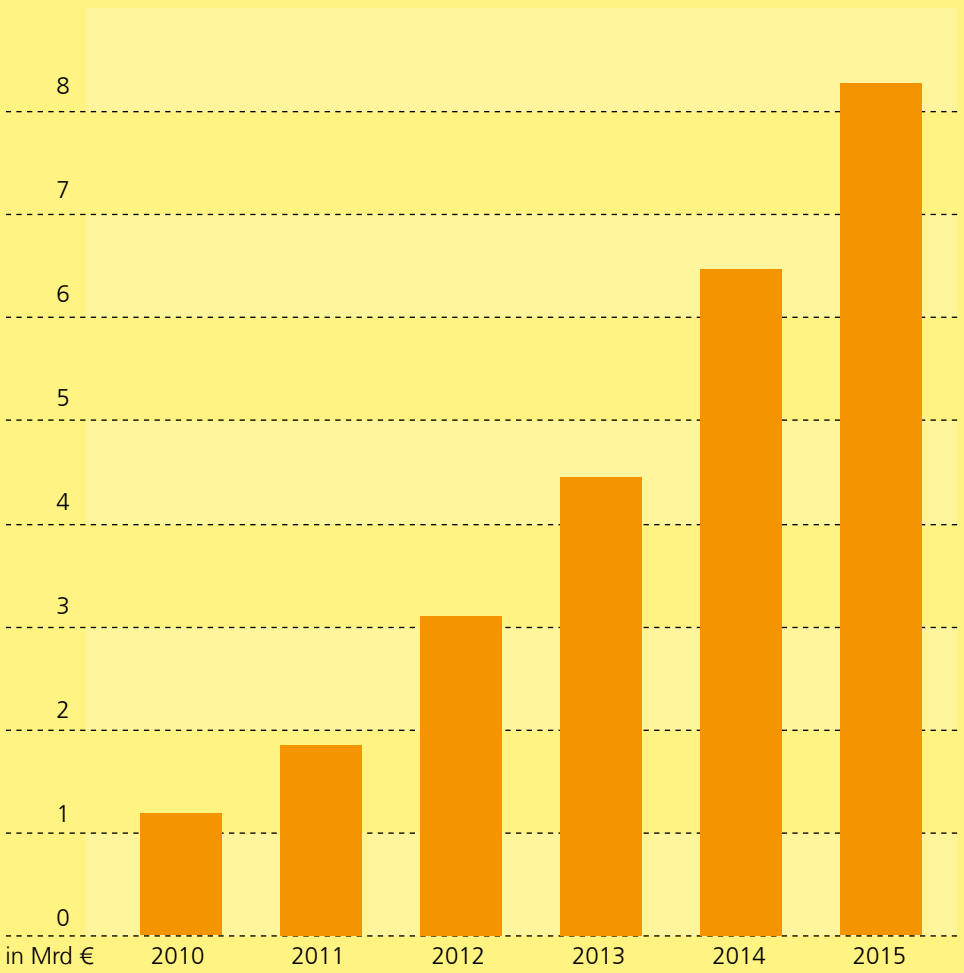
Nötig ist hierfür ein einheitlicher **technischer und juristischer Rahmen**, der Vertrauen in Cloud-Angebote schafft: Den Cloud-Nutzern muss die Sicherheit ihrer Daten gewährleistet werden sowie jederzeit Zugriff auf die eigenen Daten. Dies gilt auch bei rechtlichen Streitfragen, einem plötzlichen technischen Versagen oder einem finanziellen Bankrott des Anbieters.

Solche Rahmenbedingungen könnte eine **übergeordnete Instanz** schaffen, etwa ein Zusammenschluss von Cloud-Dienste-Anbietern oder ein Branchenverband. Dies würde viele Unsicherheiten potenzieller Kunden abbauen.

Der vorliegende Text richtet sich an europäische Unternehmen und Firmen, die Cloud-Dienste anbieten oder nutzen sowie Betriebe und Behörden, die sich für Cloud-Nutzung interessieren und sich über Risiken und Nutzen informieren möchten. Diese Zusammenfassung der Eberbacher Gespräche zeigt auf, welche Lösungen Experten aus Wirtschaft und Forschung für die gegenwärtigen »Kinderkrankheiten« des Cloud Computing vorschlagen.

UMSATZ MIT CLOUD COMPUTING IN DEUTSCHLAND

Rechnen in der Wolke



Hintergrund Cloud Computing ist ein Nutzungsmodell, das auf bestehenden und etablierten IT-Technologien beruht. Mit Cloud Computing können Unternehmen und Behörden ihre IT-Kosten reduzieren und ihre IT wesentlich flexibler gestalten: Wer Hard- oder Software in die Cloud auslagert, kann Leistungsspitzen besser abfedern sowie Beschaffungs- und Wartungskosten einsparen. Gerade kleine und mittelständische Unternehmen können sich dadurch stärker auf ihren Geschäftszweck konzentrieren und gleichzeitig ihre IT professionalisieren.

Trotz dieser Vorteile zögern viele Unternehmen noch mit dem Schritt in die Cloud. Ein wichtiger Grund hierfür sind offene Fragen zu IT-Sicherheit, Datenschutz und rechtlicher Haftungsfragen.

1 WAS IST CLOUD COMPUTING?

Cloud Computing wird gegenwärtig so viel diskutiert wie kein anderer IT-Trend, doch was sich genau hinter dem Begriff der »Cloud« verbirgt, bleibt oft nebulös. Eine schlüssige und anerkannte Definition dessen, was Cloud Computing ist, gibt das US-amerikanische National Institute of Standards and Technology NIST. Danach charakterisieren **fünf wesentliche Merkmale** das Konzept:

1. Der Nutzer kann sich selbst bedienen
Kunden eines Cloud-Dienstes können Ressourcen wie Rechenzeit oder Speicherplatz anfordern und bekommen diese automatisch zugeteilt, ohne dass ein Servicemitarbeiter das veranlassen müsste.

2. Nutzer haben Zugriff über Standardnetzwerke
Nutzer können auf die Ressourcen, die der Cloud-Anbieter zur Verfügung stellt, ausschließlich über Computernetzwerke zugreifen. Deshalb können Standardmechanismen benutzt werden und der Cloud-Dienst ist sowohl vom Smartphone als auch vom Arbeitsplatzrechner aus zu erreichen.

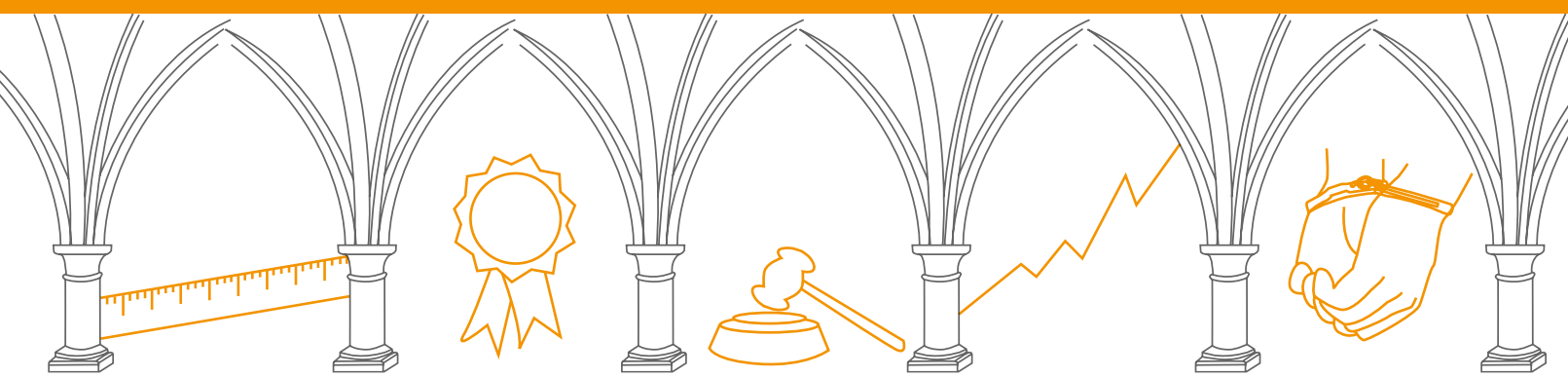
3. Nutzer teilen sich Ressourcen
Die Ressourcen, die der Cloud-Anbieter bereitstellt, sind nicht einzelnen Kunden fest zugeteilt, sondern können je nach Bedarf abgezogen oder aufgestockt werden. Diese Ressourcen können sich auch auf ein und demselben Gerät befinden, sodass verschiedene Anwendungen unterschiedlicher Nutzer dieselben Ressourcen nutzen (Multi-tenancy-Prinzip). Der Nutzer indes weiß nicht, wo sich seine Daten, Dienste, Server etc. geografisch befinden.

Diese Standortunabhängigkeit erlaubt es dem Cloud-Anbieter, seine Dienste sehr kostengünstig anzubieten. Denn er kann seine eigenen physischen Ressourcen effizienter ausnutzen als bei einer statischen Ressourcenzuteilung. Unter Umständen kann der Cloud-Dienstleister die Standortunabhängigkeit auch einschränken, sodass Ressourcen nur von einem bestimmten Standort oder Gebiet bezogen werden.

4. Nutzer bleiben flexibel
Ein Cloud-Nutzer kann gemietete Ressourcen schnell und einfach reduzieren oder erweitern, je nach aktuellem Bedarf. Dies kann auch automatisch geschehen, sodass Ressourcen – aus Sicht des Nutzers – praktisch unbegrenzt erscheinen und zu jeder Zeit nachgekauft werden können.

5. Transparenz bei Kosten und Verbrauch
Ein Cloud-Anbieter kontrolliert und misst über seine Systeme ständig den Ressourcenverbrauch, beispielsweise in Gigabyte für Speicherplatz oder in Megabit für Netzwerkbandbreite. Diese ständige Messung und Überwachung des Verbrauchs dient der Transparenz – für den Nutzer werden so die Kosten ersichtlich, für den Anbieter die Auslastung seiner Ressourcen.

2 PRAKTISCHE HERAUSFORDERUNGEN



Standards & Transparenz

Vertrauen

Rechts-sicherheit

Wirtschaftlichkeit

Abhängigkeit & Kontrollverlust

Cloud Computing birgt viele Chancen für Unternehmen und Behörden, doch zurzeit gibt es noch viele Unsicherheiten, die potenzielle Kunden abschrecken.

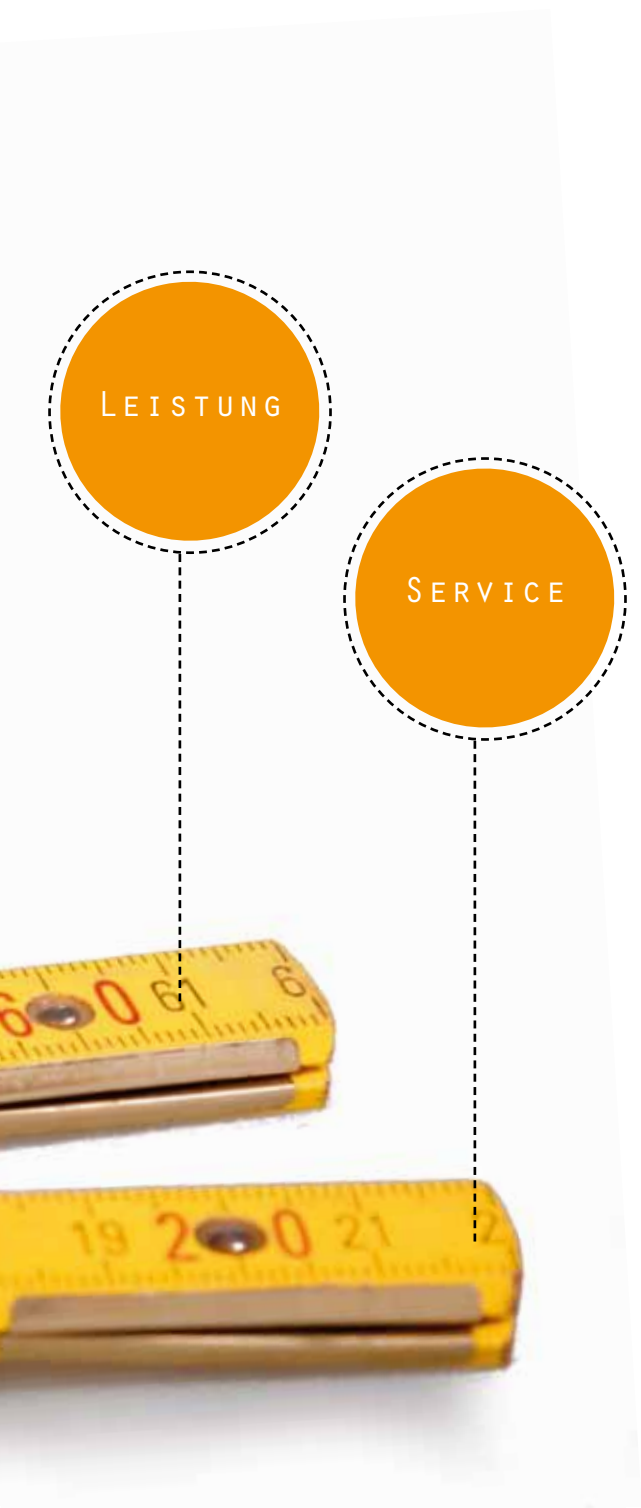
Zu den zentralen Herausforderungen zählt insbesondere die IT-Sicherheit. Damit verbunden sich technische, juristische und wirtschaftliche Aspekte, die auf den folgenden Seiten näher beleuchtet werden. Ein weiterer Punkt, der Kunden vom Schritt in die Cloud abhält, ist die Abhängigkeit von einem Cloud-Anbieter. Bislang ist noch nicht allgemeingültig geregelt, wie ein Anbieter-Wechsel reibungslos vonstatten gehen kann. Ein Hindernis ist auch der Kontrollverlust über in die Cloud ausgelagerten Daten, den Cloud-Kunden hinnehmen müssen.

KLARE MASSSTÄBE ZUM THEMA CLOUD FEHLEN

FUNKTION

SICHERHEIT

2 HERAUSFORDERUNGEN



2.1 STANDARDS UND TRANSPARENZ

Potenziellen Cloud-Nutzern ist nicht immer klar, was sie für ihr Geld bekommen. Leistungsbeschreibungen und Servicemerkmale der einzelnen Cloud-Anbieter entsprechen keiner allgemeinen Norm oder einem vergleichbaren Richtwert. Dadurch können Nutzer nur schwer erkennen, wo die Unterschiede einzelner Cloud-Angebote liegen.

Grundsätzlich ist detailliertes Wissen darüber, wie eine Cloud arbeitet, nicht erforderlich – Autofahrer wissen in der Regel auch nicht genau, wie ihr Wagen und dessen Motor funktionieren und können das Auto dennoch problemlos benutzen. Auch lassen sich Fahrzeuge verschiedener Hersteller anhand standardisierter Merkmale wie Kraftstoffverbrauch, Leistung oder CO_2-Ausstoß leicht vergleichen. Für Cloud Computing fehlen noch ähnliche **Erfahrungswerte, akzeptierte Vergleichsmodelle sowie allgemeine, einheitliche Standards** und Merkmale, an denen sich Kunden orientieren können. Für einzelne Dienstmerkmale wie Sicherheit und Funktionalität, gibt es **keine verbindlichen Richtwerte oder Skalen**. Deshalb lassen sich Angebote verschiedener Cloud-Dienstleister schwer vergleichen.

VERTRAUEN

Gegenseitigkeit, Kompetenz, Vergleichbarkeit, Wohlwollen, Integrität, Berechenbarkeit, Sicherheit, Einbindung, Offenheit mit Informationen, Erreichbarkeit. Zehn Faktoren, die das Vertrauen in Teams erhöhen und auch im Kundenverhältnis wichtig sind. Die Grafik zeigt ein Beispiel, wie hoch oder niedrig die einzelnen Komponenten ausgeprägt sein können.

GEGENSEITIG

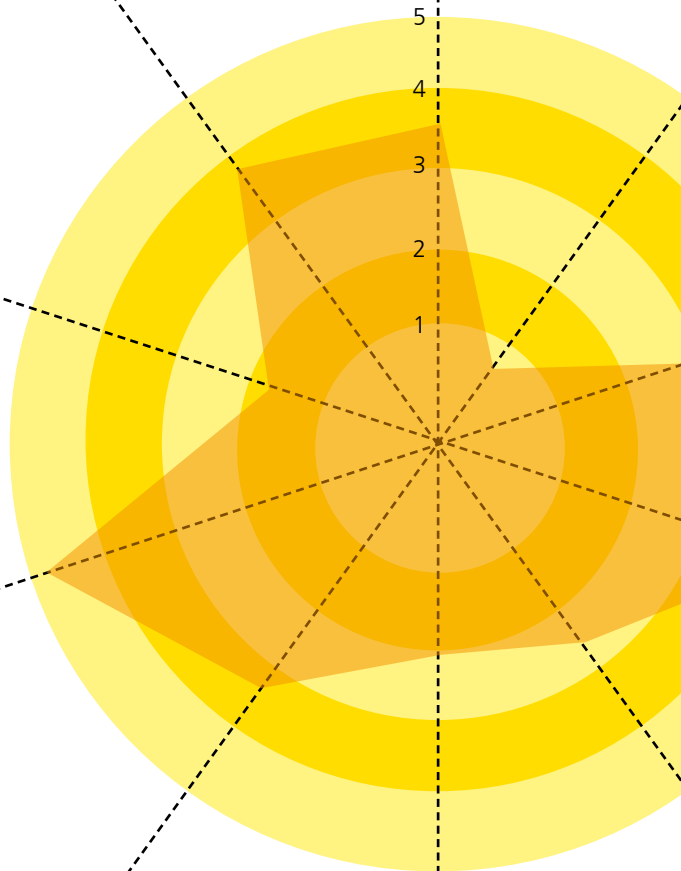
KOMPETENT

ERREICHBAR

OFFEN MIT INFORMATION

EINBEZIEHEND

SICHER



Quellen: www.ecbproject.org/the-ten-criteria-for-trust/the-ten-criteria-for-trust; www.worldwork.biz/legacy/www/docs2/te

2 HERAUSFORDERUNGEN

KOMPATIBEL

WOHLWOLLEND

INTEGER

VORHERSEHBAR

2.2 MANGELNDES VERTRAUEN

Unternehmen oder Behörden, die Cloud-Angebote nutzen, besitzen wesentlich weniger Informationen über ihre Daten und deren Sicherheit als der Anbieter. Sicherheitsgarantien, die bislang häufig auf Selbsteinschätzungen der Anbieter beruhen, sind kaum nachzuprüfen. Auf einer solchen Basis ist es deshalb für Nutzer nur schwer möglich, einem Anbieter zu vertrauen.

Ein Ansatz diesem Problem zu begegnen sind **Zertifikate**: Einige Cloud-Anbieter lassen Zertifizierungen ihrer Dienste durchführen, beispielsweise nach Standard SAS 70 (wurde ersetzt durch SSAE 16) oder ISO 27001. Diese definieren zumeist jedoch nur eine Untergrenze in Hinblick auf Sicherheit. Wie sicher die Daten der Nutzer tatsächlich sind, hängt davon ab, wie der Anbieter die Sicherheitsmaßnahmen konkret umsetzt. Zwei Anbieter mit derselben Zertifizierung können ganz unterschiedliche Sicherheitsniveaus besitzen. Beispielsweise kann ein Anbieter zur Sicherung seiner IT-Infrastruktur eine Firewall installiert haben, während ein anderer neben der Firewall auch eine Demilitarisierte Zone (DMZ), also ein Netzwerk zwischen Internet und internem Netzwerk, und intrusion detection system (IDS), ein Angriffserkennungssystem, eingerichtet hat. Damit erreicht der zweite Anbieter ein grundsätzlich höheres Sicherheitsniveau. Ob dies für den Anwendungsfall sinnvoll ist, ist damit aber nicht gesagt – die Schutzmaßnahmen könnten auch völlig übertrieben sein. Um die Sicherheit eines Cloud-Dienstes realistisch einschätzen zu können, müssten Nutzer zusätzlich die Bewertungsberichte der Zertifizierer prüfen, anhand derer sich erkennen lässt, welche Maßnahmen konkret der Cloud-Anbieter getroffen hat. Diese Berichte sind für IT-Security-Laien unverständlich.

Deutsches Datenschutzrecht

Das deutsche Datenschutzrecht unterscheidet zwischen dem Sitzland- und dem Territorialprinzip: Hat ein Cloud-Dienste-Anbieter seinen Sitz innerhalb des Europäischen Wirtschaftsraumes (EWR), so richtet sich das anzuwendende Datenschutzrecht nach dem Sitz des Cloud-Dienste-Anbieters (=Sitzlandprinzip). Für deutsche Anbieter gelten also die deutschen Datenschutzregelungen, für spanische Anbieter die spanischen Regelungen etc.

Hat ein Cloud-Dienste-Anbieter eine Niederlassung in Deutschland, in der Daten verarbeitet werden, so finden die deutschen Datenschutzregelungen Anwendung (=Territorialprinzip). Das Territorialprinzip wird auch auf Unternehmen angewandt, die in Deutschland Daten erheben, aber keine Niederlassung innerhalb des EWR haben. Dies gilt auch für die USA, wo einige der grössten Cloud-Anbieter weltweit sitzen.

2 HERAUSFORDERUNGEN

Zudem stellen die Zertifikate die Sicherheit meist aus Anbietersicht dar. Die Nutzersicht kann sich davon erheblich unterscheiden: Der Anbieter selbst sieht sich typischerweise nicht als möglichen Angreifer, deshalb zielen Sicherheitsmaßnahmen oft nur darauf, einen Schutz gegenüber Dritten zu gewährleisten. Nutzer könnten aber auch einen Schutz vor Datenmissbrauch gegenüber dem Anbieter fordern, etwa dadurch, dass Daten nur verschlüsselt abgelegt werden und der Anbieter den Schlüssel nicht kennen darf. Problematisch wäre es beispielsweise, wenn Anbieter ohne Wissen und Einfluss des Nutzers auf dessen Daten zugreifen könnten.

Eine weitere Möglichkeit, das Vertrauen von Kunden in die Sicherheit von Cloud-Diensten zu fördern, ist der Einsatz von **Verschlüsselungstechnologie**. Doch auch hier ist unklar, wie genau Nutzerdaten geschützt werden. Zwar werben manche Anbieter mit »starker Verschlüsselung«. Damit meinen sie aber oft lediglich eine Absicherung der Kommunikation, also eine verschlüsselte Verbindung. Diese schützt die Daten jedoch lediglich auf dem Transportweg in die Wolke. Selbst bei einer Verschlüsselung der Daten, die auf dem Nutzerrechner oder in der Cloud durchgeführt wird, kennt der Anbieter aber typischerweise den Schlüssel für die Entschlüsselung. Für Nutzer stellt sich deshalb weiter die Frage, ob die Daten vertraulich gehalten werden, aber auch, wie die Daten vor Diebstahl von extern oder intern geschützt werden.

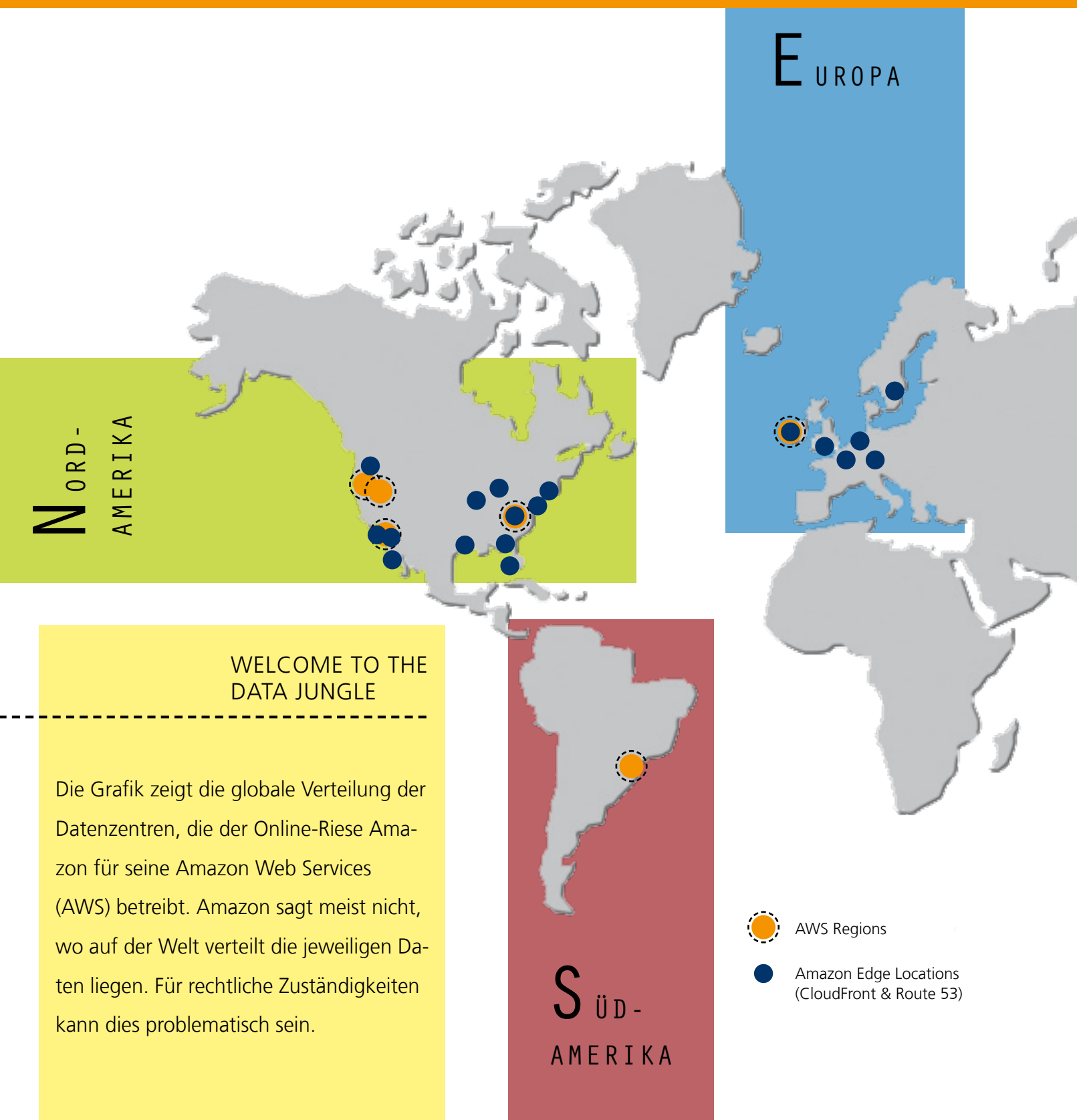
Noch fehlt es also an Möglichkeiten, ausreichendes Vertrauen in die technische Sicherheit von Cloud-Angeboten herzustellen.

2.3 FEHLENDE RECHTSSICHERHEIT

Typisch für Cloud Computing ist, dass es Nutzern selten ganz klar ist, wo im geografischen Sinne ihre Informationen in der Datenwolke gespeichert sind. Deshalb ist es mitunter schwierig festzustellen, welches das **anzuwendende Rechtssystem** ist – das Recht des Landes, in dem der Nutzer ansässig ist, oder das Recht des Landes, in dem der Anbieter seinen Sitz hat. Besonders problematisch ist dies, wenn die Regelungen des Anbietersitzlandes im Widerspruch zu den Gesetzen des Nutzerlandes stehen.

Aktuelle **Cloud-Geschäftsmodelle** berücksichtigen diese juristischen Unterschiede nicht ausreichend. Vielmehr verfolgen die Anbieter den Gedanken eines Einheitsdienstes nach dem Motto **»one size fits all«**. Individuelle Verträge zwischen Cloud-Anbieter und Nutzer hinsichtlich Speicherung, Verarbeitung und Nutzung von Daten in der Wolke sind in der Regel nicht möglich. Für die Anbieter bedeutet diese Vereinfachung eine höhere Effizienz und damit Kosteneinsparungen, die sie an ihre Kunden weitergeben können. Die Gefahr bei diesem Geschäftsmodell insbesondere für deutsche Unternehmen ist, dass die Firmen durch Nutzung des Cloud-Dienstes unter Umständen gegen rechtlichen Pflichten verstoßen.

Augenscheinlich wird dieses Problem beim Thema **Datenschutz**. Das deutsche Datenschutzrecht setzt im Gegensatz zu anderen Staaten hohe Maßstäbe an, was den Schutz personenbezogener Daten angeht. Doch deutsches Datenschutzrecht lässt sich in der Praxis schwer durchsetzen, wenn die Gesetze des Landes, in dem der Anbieter seinen Sitz hat, im Widerspruch zu deutschen Gesetzen oder Richtlinien der EU stehen.



WELCOME TO THE DATA JUNGLE

Die Grafik zeigt die globale Verteilung der Datenzentren, die der Online-Riese Amazon für seine Amazon Web Services (AWS) betreibt. Amazon sagt meist nicht, wo auf der Welt verteilt die jeweiligen Daten liegen. Für rechtliche Zuständigkeiten kann dies problematisch sein.

2 HERAUSFORDERUNGEN

Ein deutsches Unternehmen, das Cloud-Dienste nutzen möchte, läuft also Gefahr, seine Datenschutz-Pflichten nicht einhalten zu können. Diese Pflichten lassen sich nicht einfach an den Cloud-Dienst-Betreiber weitergeben, weil der Nutzer nicht prüfen kann, ob der Anbieter die gesetzlichen Bestimmungen einhält – und eine Selbsteinschätzung des Dienste-Anbieters in der Regel nicht ausreicht. Wenn der Nutzer beispielsweise Daten seiner Kunden weitergibt, müssen Anbieter und Nutzer vertraglich festlegen, wie die Daten behandelt werden. Dies gestaltet sich aber schwierig, da das Vertragsverhältnis zwischen Anwender und Anbieter in dieser Hinsicht unvollständig beschrieben ist. So haftet der Cloud-Nutzer gegenüber seinen Kunden bei mangelhafter Leistung des Dienstanbieters, etwa bei unsicherer Datenhaltung. Denn der Cloud-Nutzer ist seiner Sorgfaltspflicht nicht hinreichend nachgekommen.

Zurzeit gibt es also ein Spannungsfeld zwischen dem unternehmerischen und finanziellen Potenzial, das Cloud Computing für Unternehmen bietet, auf der einen Seite und den rechtlichen Rahmenbedingungen auf der anderen Seite. Dies führt in der Praxis zu Unsicherheiten und Zurückhaltung bei potenziellen Cloud-Nutzern.

Die Auswirkungen auf in Deutschland ansässige Cloud-Anbieter sind zwiespältig: Einerseits leiden auch sie unter einem generellen Misstrauen gegenüber Cloud-Dienstleistern, besonders, wenn in diesem Zusammenhang in den Medien über Datenskandale berichtet wird. Andererseits müssen Cloud-Anbieter mit Sitz in Deutschland automatisch höchsten Datenschutzanforderungen genügen, was besonders für Unternehmen attraktiv ist, die personenbezogene Daten – etwa Personalinformationen – auslagern wollen.

Quelle: http://www.theregister.co.uk/2012/01/06/amazon_aws_biz_2011/print.html

» 50% DER KLEINEN UND MITTLEREN UNTERNEHMEN HABEN KEINEN NOTFALL- BZW. BACK-UP-PLAN, 41% HABEN SICH NOCH NICHT MAL GEDANKEN ÜBER DIE NOTWENDIGKEIT EINES SOLCHEN PLANS GEMACHT. «

SYMANTEC, 2011

» BEIM CLOUD COMPUTING BESITZT DER CLOUD-NUTZER WESENTLICH WENIGER INFORMATIONEN ZU SEINEN DATEN UND DEREN SICHERHEIT ALS DER CLOUD-ANBIETER. DIE HÄUFIG AUF SELBSTEINSCHÄTZUNG DES ANBIETERS BASIERENDEN GARANTIEN KÖNNEN NUTZER NUR SCHWER NACHPRÜFEN. «

MICHAEL WAIDNER, FRAUNHOFER SIT

2 HERAUSFORDERUNGEN

2.4 WIRTSCHAFTLICHKEIT

Sicherheit um jeden Preis ist wirtschaftlich nicht sinnvoll. Jedes Unternehmen sucht dementsprechend die Balance zwischen Sicherheit und deren Kosten. Grundsätzlich wünschen sich die meisten Cloud-Nutzer vermutlich, dass ihre Daten in der Cloud ebenso gut gesichert sind wie auf eigenen, selbst kontrollierten Geräten oder einer eigenen Infrastruktur.

» IF YOU TAKE A BROAD ENOUGH DEFINITION OF TRUST, THEN IT WOULD EXPLAIN BASICALLY ALL THE DIFFERENCE BETWEEN THE PER CAPITA INCOME OF THE UNITED STATES AND SOMALIA. «

STEVE KNACK, A SENIOR ECONOMIST AT THE WORLD BANK

Mehr Sicherheit für Kleine

Gerade bei kleinen und mittleren Unternehmen (KMU) mit eigener Infrastruktur kann die Cloud-Nutzung mehr Sicherheit zu geringeren Kosten bringen. Das ist beispielsweise der Fall, wenn ein KMU keine Vollzeit-IT-Administration besitzt, der Cloud-Anbieter hingegen für die Instandhaltung und Wartung seiner Infrastruktur geschultes Vollzeit-Personal einsetzt.

Weniger Sicherheit für Große

Unternehmen, die qualifiziertes Personal zur Absicherung ihrer eigenen Strukturen einsetzen, werden beim Schritt in die Cloud hingegen versuchen, ihre bisherigen Sicherheitsstandards zu halten. Anders als beim herkömmlichen Auslagern von Diensten wird es beim Cloud Computing nicht möglich sein, den Anbieter auf die Einhaltung der eigenen Sicherheitsrichtlinien zu verpflichten – dies widerspricht dem Geschäftsmodell »one size fits all« (s. vorheriger Abschnitt). Microsoft weist beispielsweise in seinen FAQ, die auch für Microsofts Azure-Cloud gelten, explizit darauf hin, dass ausschließlich die Einhaltung der Microsoft-Sicherheitsrichtlinie gewährleistet wird und nicht etwa die des Kunden.

Potenzielle Cloud-Nutzer müssen also prüfen, welches Sicherheitsniveau der Cloud-Anbieter garantiert. Etwa wie Übermittlung und Zugriff auf die Daten gesichert sind und wie die Vertraulichkeit der Daten bei Nutzung und Transport technisch und organisatorisch sichergestellt wird. Fällt diese »Sicherheitsbilanz« zu Ungunsten des Anbieters aus, kann sich der Nutzer entweder einen anderen Cloud-Anbieter suchen. Oder er kann selbst das Sicherheitsniveau durch zusätzlichen Aufwand erhöhen, was aber Effizienz und Einsparungen verringert.

KONTROLLVERLUST – WER SICH AUF DIE CLOUD VERLÄSST, MACHT SICH AUTOMATISCH ABHÄNGIG VOM JEWEILIGEN ANGEBOT

2 HERAUSFORDERUNGEN

2.5 ABHÄNGIGKEIT UND KONTROLLVERLUST

Wer wichtige Daten und Prozesse zu einem Dienstleister auslagert, macht sich automatisch abhängig von diesem Anbieter. Das gilt beim Cloud Computing ebenso wie beim klassischen IT-Outsourcing. Beim Cloud Computing hat der Nutzer jedoch weniger konkrete Informationen darüber, wie und wo die eigenen Daten gespeichert werden und wer konkrete Ansprechpartner für die eigenen Daten und Prozesse sind. Hinzu kommen beim Cloud Computing unter Umständen verdeckte Abhängigkeiten. Dies kann etwa der Fall sein, wenn ein Cloud-Anbieter keine eigene Infrastruktur betreibt, sondern hierfür auf die Infrastruktur eines anderen Anbieters zurückgreift. Dies ist beispielsweise der Fall beim Anbieter Dropbox, dessen Backend auf Amazons Dienst S3 beruht.

Technisches und finanzielles Versagen

Darüber hinaus besteht auch ein übergreifendes Risiko: Wenn nämlich scheinbar viele Cloud-Anbieter ihre Dienste anbieten, dahinter aber tatsächlich nur einige wenige große Anbieter stehen, die eine eigene Infrastruktur betreiben. Versagt ein solcher Anbieter, könnte das zu einem systemischen Zusammenbruch führen: Im schlimmsten Fall wären damit Wirtschaft und Gesellschaft eines Landes bedroht. Die Gründe für ein solches Versagen eines großen Cloud-Anbieters können technisch oder wirtschaftlich sein:

- **Technisch** kann es passieren, dass ein Cloud-Angebot schlicht nicht erreichbar ist, sodass der Nutzer bestimmte Arbeitsprozesse nicht mehr durchführen oder dass er nicht mehr auf Daten zugreifen kann.
- Ein **finanzieller** Ausfall eines Cloud-Anbieters, beispielsweise durch Insolvenz, tritt womöglich nicht so plötzlich ein wie technisches Versagen. Trotzdem kann dies unter Umständen so kurzfristig eintreten, dass ein rechtzeitiger Rückzug oder Umzug aus der Cloud nicht mehr möglich ist.

FAZIT

Mangelndes Vertrauen in das Angebot der Cloud-Anbieter scheint derzeit das größte Problem zu sein, das potenzielle Firmenkunden bislang davon abhält, die Cloud-Technologie für sich zu nutzen. Hier lassen sich grob zwei Bereiche unterscheiden:

- Es fehlt das Vertrauen der Nutzer in Hinblick auf die ständige Verfügbarkeit ihrer Daten in der Cloud (Sicherheit bei technischem oder wirtschaftlichem Kollaps) – Kunden wissen nicht, ob und wie sie an ihre Daten gelangen können, wenn der Cloud-Anbieter – aus welchen Gründen auch immer – nicht mehr verfügbar ist.
- Es fehlt das Vertrauen der Nutzer hinsichtlich Datensicherheit und ausreichendem Datenschutz seiner ausgelagerten Daten und Prozesse.

Die zentrale Frage ist also, wie Anbieter mehr Vertrauen in ihr Angebot schaffen können. Im Folgenden werden Lösungsansätze für die einzelnen Probleme vorgestellt.

3 LÖSUNGSANSÄTZE

3.1 SICHERUNGSINSTANZ BEI TECHNISCHEM VERSAGEN

Was passiert, wenn ein Cloud-Angebot technisch nicht mehr erreichbar ist? Ein Blick in andere Branchen zeigt, dass es beispielsweise bei Banken, Versicherungen, Energieversorgern oder Krankenkassen für solche Situationen Sicherungsmechanismen gibt: Bei den Banken greifen Einlagensicherungsfonds, Versicherte einer insolventen Krankenkasse müssen von einer anderen Kasse aufgenommen werden, und beim Ausfall eines Energieversorgers übernimmt der sogenannte Grundversorger die Leistung. Vergleichbare **Sicherheitsvorkehrungen** im Cloud-Umfeld würden dazu beitragen, ein größeres Vertrauen der Nutzer zu etablieren.

Ähnlich wie beim Bankenmodell könnten die deutschen Cloud-Anbieter gemeinsam eine Sicherungsinstanz einrichten. Denkbar wäre etwa eine Gesellschaft deutscher Cloud-Anbieter, die bei technischem Versagen eines Mit-Anbieters einspringt und einen Basisbetrieb der Dienste sicherstellt (business continuity). Diese Sicherungsinstanz müsste in das Dienste-Angebot und die allgemeinen Geschäftsbedingungen jedes deutschen Cloud-Providers aufgenommen werden.

Juristisch wäre zu klären, wie ein Transfer von einem insolventen Cloud-Provider hin zur Not-Sicherungsinstanz rechtlich so gestaltet werden kann, dass keine Konflikte mit Gesetzen und Verordnungen unterschiedlicher Länder entstehen. Man müsste außerdem klären, welches Haftungsrisiko für den Cloud-Nutzer entsteht. Beispielsweise müsste in Verträgen zwischen Nutzer und Anbieter klar dargestellt werden, wie der Cloud-Anbieter mit personenbezogenen Daten von Kunden des Nutzers umgeht (s. Punkt 2.3).

Technisch fehlen bislang gemeinsame und offene Standards auf Anbieterseite. Hier gilt es, solche **Standards und Schnittstellen** zu entwickeln, um im Notfall einen reibungslosen und schnellen Transfer zu ermöglichen (siehe auch nächsten Punkt).

Wenn dies alles berücksichtigt und eingeführt wird, ließe sich bei einem eingetretenen oder absehbaren Kollaps eines Cloud-Dienstes ein technisch und juristisch einwandfreier Transfer der Kundendaten und -prozesse realisieren. Ein weiteres Plus von gemeinsamen Standards und Rechtssicherheit wären Wettbewerbsvorteile deutscher Cloud-Anbieter gegenüber Konkurrenten – über Standards werden Angebote besser vergleichbar. Rechtssicherheit auch in Fällen von Insolvenz wäre ein Wettbewerbsvorteil deutscher Anbieter gegenüber ausländischer Konkurrenz. Eine **»Cloud made in Germany«** könnte sich deshalb als Gütesiegel etablieren. Für interessierte Nutzer hat der ITK-Branchenverband BITKOM[1] bereits ein Anbieterverzeichnis von deutschen Cloud-Dienstleistern erstellt. Auf europäischer Ebene schlagen SAP und Roland Berger in einer Studie von 2011[2] einen sogenannten »European Cloud Gold Standard« vor.

1 die Aufstellung deutscher Cloud-Anbieter findet sich hier: http://sit4.me/Bitkomcloud
2 http://sit4.me/SAP-Berger

STANDARD IN DEN BESCHREIBUNGEN + GEMEINSAME SCHNITTSTELLE + DEN ÜBERBLICK BEHALTEN

BEIM DATENTRANSFER KÖNNEN DURCH STANDARDS UND CHECKLISTEN HÖHERE SICHERHEITSWERTE ERREICHT WERDEN

3 LÖSUNGSANSÄTZE

3.2 EINFÜHRUNG GEMEINSAMER STANDARDS UND CHECKLISTEN

Zurzeit kostet ein Cloud-Provider-Wechsel den Kunden viel Zeit und Geld, da es eine Vielzahl unterschiedlicher Schnittstellen gibt. Das verhindert einen Transfer von Daten. Für einen **gemeinsamen Schnittstellenstandard** müssen zunächst Basisschnittstellen definiert werden, welche den Transfer von Daten und Prozessen von einem Cloud-Anbieter zum anderen in einer Standardprozedur ermöglichen. Ein denkbares Forum für die Entwicklung und Beförderung von Standards oder von Leitfäden hierfür wären in Deutschland der BITKOM oder internationale Organisationen wie die IETF (Internet Engineering Task Force), das W3C (World Wide Web Consortium) oder OASIS (Organization for the Advancement of Structured Information Standards). Infrage käme auch die Cloud Security Alliance (CSA), der Auditierer-Verband ISACA oder die Europäische Agentur für Netz- und Informationssicherheit (ENISA).

Wo zusätzliche Schnittstellen sinnvoll erscheinen, kann man auch **branchenspezifische Ergänzungen** definieren. Beispielsweise könnten Banken- oder Bildungs-Clouds eine gemeinsame Basisschnittstelle besitzen, darüber hinaus aber weitere Schnittstellen, die jeweils auf spezifische Anwendungen ausgerichtet sind.

Für eine Vergleichbarkeit von Cloud-Diensten reichen standardisierte Schnittstellen allein aber nicht aus. Unternehmen und Behörden, die einen Anbieter suchen, müssen eigenständig eine sinnvolle und passende Wahl treffen können. Deshalb sollten zum einen **Bedarfs-Checklisten** für Nutzer erstellt werden, mit denen potenzielle Kunden zunächst die für sie wichtigen Merkmale feststellen können. Zum anderen sollte eine **standardisierte Beschreibung** von Angeboten aufgestellt werden. Anhand dieser Beschreibung könnten Nutzer unterschiedliche Cloud-Angebote mit wenig Aufwand vergleichen.

3.3 VERSTÄNDLICHKEIT

Datenschutz und Datensicherheit sind komnplexe Themen. Es ist schwierig zu vermitteln, wer was wann genau zu beachten hat. Das ist auch im Cloud-Umfeld nicht anders. Die meisten Cloud-Anbieter behandeln in ihren AGBs und Angeboten jedoch gerade diese für Nutzer so wichtigen Themen eher stiefmütterlich. Viele Anbieter gehen entweder gar nicht darauf ein oder beschreiben ihre Sicherheitsmaßnahmen nur oberflächlich oder schwer verständlich. Das erschwert es Nutzern, Vertrauen zu fassen. Cloud-Anbieter sollten in allgemein verständlicher Sprache beschreiben, welche Sicherheitsmaßnahmen sie vornehmen. So können potenzielle Kunden erkennen, wie ihre Daten geschützt werden. Beispielsweise könnten Anbieter – ohne sich in technischen Details zu verlieren – erklären, ob Daten von Nutzern ungeschützt in die Cloud gelangen, ob die Daten nur während des Transports vor der Einsicht durch Dritte geschützt sind, oder ob Daten prinzipiell selbst für den Anbieter selbst nicht einsehbar sind.

Basissicherheit

Wie genau ist der Zugriff auf die Daten abgesichert? Kann jeder, der eine bestimmte Internetadresse kennt, die Daten einsehen? Wird ein Passwort benötigt? Oder kommen professionellere Verfahren zum Einsatz, wie Authentifizierung über Zertifikate? Gibt es gar neuartige Schutzverfahren wie die eID-Funktion des neuen Personalausweises? Sicherlich wird nicht jeder Nutzer die Abstufungen der unterschiedlichen Verfahren kennen. Es könnten jedoch verschiedene Sicherheitsstufen klassifiziert werden (niedrig, mittel, hoch, Skala 1 bis 6 oder ähnliches), die auch Nichtexperten einen greifbaren Eindruck des Sicherheitsniveaus vermitteln. Eine solche Einteilung – beispielsweise durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) – würde sich schnell durchsetzen und weithin anerkannt.

MEHR SICHERHEIT

Jedes Extra lässt die Bewertung steigen.

AIRBAG

LICHT

3 LÖSUNGSANSÄTZE

Datenschutz-Audits

Schutzmaßnahmen vor Zugriff und Schutz der Vertraulichkeit von Daten gegenüber Dritten sind ein wichtiger Aspekt von Sicherheit, meinen aber nicht dasselbe wie Datenschutz. Die Erklärung eines Anbieters stellt keine ausreichende Garantie dar, dass Nutzerdaten in der Praxis auch wie versprochen behandelt werden. Dieses Problem besteht jedoch nicht nur für das Cloud Computing, sondern auch in anderen Bereichen. Um hier zusätzliches Vertrauen aufzubauen, können Audits von unabhängigen Dritten bestätigen, dass Cloud-Anbieter gegebene Garantien oder Gesetze einhalten. Dieses Modell hat sich beispielsweise bei Wirtschaftsprüfungen etabliert und könnte in abgewandelter Form auch auf Anbieter von Cloud-Diensten angewandt werden.

4 FAZIT

GEWINNER DES WETTBEWERBS »TRUSTED CLOUD« DES BMWI

Verbesserungen in den zuvor genannten Bereichen können helfen, Unternehmen den Weg in die Cloud zu ebnen und sie dabei unterstützen, das Potenzial von Cloud Computing zu nutzen. Besonders Unternehmen, die bislang nicht oder nur sehr zögerlich Cloud-Technologie einsetzen, könnten hiervon profitieren. Für Cloud-Anbieter bietet sich gleichzeitig die Chance, durch Standardisierung, Datenschutz-Audits und konstruktiven Umgang mit den Sicherheitsfragen ihre Dienstangebote so weiter zu entwickeln, dass Bedenken von Nutzern abgebaut werden. Damit wird die Nachfrage nach dem eigenen Dienstangebot gefördert. Insbesondere deutsche Unternehmen haben die Möglichkeit, sich über gesetzlich vorgeschriebene strenge Sicherheits- und Datenschutzvorschriften Alleinstellungsmerkmale und damit Marktvorteile zu sichern.

SEALED CLOUD
Versiegelte Infrastruktur für Cloud Computing, die Daten und Anwendungen gegen externe und interne Angriffe und Missbrauch schützt

SKIDENTITY
Erstellt ‚Identity Broker', der Cloud-Computing-Infrastrukturen mit Authentifizierung des neuen Personalausweises verbindet

VALUE4CLOUD
Mehrwertdienste zur Förderung von Qualität und Vertrauen in Cloud Computing

MIA
Vertrauensvolle Cloud-Plattform zur Informationsanalyse und zum Informationsmanagement

CLOUD4E
Simulationswerkzeuge als Dienst für die Produktentwicklung

PEERENERGYCLOUD
Nutzung von Cloud Computing für Steuerungs- und Optimierungsprozesse im Smart Grid

SENSORCLOUD
Plattform zur multidimensionalen Analyse und Nutzung von Sensordaten

GENECLOUD
Cloud-Anwendungen, die mittelständische Pharma-Unternehmen beim Wirkstoff-Screening unterstützen

HEALTHCLOUD
Cloud-Dienste, die auf der Sekundärnutzung klinisch-ärztlicher Routinedaten basieren

TRESOR
Aufbau eines Cloud-Ecosystems, um medizinische Verlaufsdokumentationen effizient zu nutzen

CLOUDCYCLE
Open-Source-Cloud-Plattform für Schulverwaltung und Bürgerportale

GOBERLIN
Plattform zur Entwicklung von innovativen Apps für Bürger, Wirtschaft und Verwaltung

Quelle: BMWi

Redaktion
Michael Waidner, Michael Herfert,
Matthias Enzmann, Oliver Küch

Layout
Mona Bien

Anschrift der Redaktion
Fraunhofer SIT
Presse- und Öffentlichkeitsarbeit
Rheinstraße 75
64295 Darmstadt
Telefon +49 6151 869-282
Fax +49 6151 869-224

redaktion@sit.fraunhofer.de

Bildquellen
iStock: S1, S.6, S.10, S.12,
S.16/17, S.18, S.26, S.30, S.34
Fotolia: S.16/17, S.24
MEV: S.8/9
Getty images: S.32
Alle anderen Abbildung:
©Fraunhofer

WEITERFÜHRENDE LINKS

Guiding Principles for Cloud Computing Adoption and Use
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use.aspx

Towards a European Cloud Computing Strategy
http://ec.europa.eu/information_society/activities/cloudcomputing/index_en.htm