(Gar) Keine Daten in die Cloud!?
Was geht wirklich (nicht)?

Stefan Kinnen
Apps Associates GmbH
Dortmund

Schlüsselworte
Cloud, Datenschutz, IT-Sicherheit.

Einleitung
Die Gehaltsabrechnung kommt via SaaS aus dem Web und Onlinebanking geschieht via Tablet oder Smartphone. Privat ist Cloud-Nutzung weit akzeptiert. Betriebliche Marketing- oder Personalabteilungen nutzen ebenfalls schon fleißig Cloud Services. In der IT ist die Zurückhaltung noch immer groß.
Eine Meinung zu Cloud Computing haben viele heute schnell gefasst. Was sind aber eigentlich die gesetzlichen Rahmenbedingungen? Was sagt der Datenschutz wirklich?
Was empfehlen die führenden Branchenverbände BITKOM und VOICE in ihren Positionspapieren zu Cloud Computing und zur deutschen Cloud-Standortpolitik?
Wo liegen heute die Grenzen und worauf kann sich die IT langfristig wohl einstellen?
In seinem Vortrag liefert Stefan Kinnen Fakten, stellt aus der Praxis einige Go's und No-Go's vor und versucht heutige und künftige Grenzen zu ziehen

Zusammenfassung aus dem BITKOM Cloud Monitor (2015)

„Cloud-Nutzung wächst – Sicherheitsbedenken bremsen“ so fasst die BITKOM basierend auf einer Studie der KPMG den Cloud Jahresbericht 2015 zusammen. Im Jahr 2014 ist demnach die Zahl der Cloud-Nutzer in Deutschland weiter gestiegen. Mittlerweile setzen fast die Hälfte der deutschen Unternehmen Cloud-Services ein. Sicherheitsbedenken bleiben die größte Hürde, die einer (intensiveren) Cloud-Nutzung im Wege stehen. Darauf reagieren die Anbieter beispielsweise mit dem Aufbau von Rechenzentren in Deutschland. Die BITKOM geht in ihrer Studie davon aus, dass sich der Business Case für Cloud-Computing gerade in Verbindung mit anderen Mega-trends wie Big Data und Mobility zukünftig noch stärker herauskristallisieren wird.

Begründet sind diese Sicherheitsbedenken nicht!

Einige Kennzahlen untermauern, dass diese oft spontan geäußerte Grundhaltung nicht objektiv begründet werden kann.

1. Die Nutzung von Cloud Diensten wächst weiter
   44% der Unternehmen in Deutschland setzen bereits Cloud Computing ein – weitere 24% erwägen es

2. 85% der registrierten IT-Angriffe auf Unternehmen haben nichts mit Cloud Computing zu tun

3. 78% der Private Cloud Nutzer bewerten ihre Erfahrungen als positiv

4. Nur 8% der Cloud Benutzer berichten über Compliance Vorfälle in Zusammenhang mit der Cloud

5. 74% der Unternehmen versprechen sich von Private Cloud Diensten einen verbesserten Zugriff auf IT Ressourcen und auch 75% bestätigen, dass dieses Ziel erreicht wurde

Auffallend ist noch eine andere Zahl: 71% der Unternehmen, die Private Cloud Services eingeführt haben, gaben als Ziel eine Erhöhung der Datensicherheit an!

Basierend auf Sicherheitsbedenken bleibt aber weiterhin die Kernforderung von 83% der deutschen Cloud Kunden an ihren Cloud Provider, dass die Rechenzentren in Deutschland betrieben werden.

(Quelle: BITKOM / KPMG Cloud Monitor 2015)

Oracle eröffnet zwei Rechenzentren in Deutschland

Um diesen breiten Kundenerwartungen gerecht werden zu können, hat Oracle im Februar 2015 in Frankfurt am Main und München die ersten Cloud-Rechenzentren in Deutschland eröffnet. Mit Frankfurt als Produktions- und München als Backup-Rechenzentrum bietet Oracle nun auch deutschen Unternehmen eine lokale Cloud-Infrastruktur und erlaubt es Kunden, ihre IT-Aufgaben auch aus der Cloud datenschutzkonform abzubilden.

In den neuen Rechenzentren werden jedoch zunächst nur die Produkte Oracle ERP Cloud, Oracle Sales Cloud, Oracle HCM Cloud, Oracle Talent Management Cloud und Oracle Service Cloud bereitgestellt. Weitere Cloud Services werden folgen.

Sicherheit, Datenschutz und Standort der Cloud sind von größter Bedeutung für Kunden aus Deutschland – die neuen Oracle Cloud Rechenzentren in Frankfurt und München tragen diesen Bedürfnissen Rechnung. Die Datenschutzbestimmungen der Europäischen Union (EU) gehören zu den strengsten weltweit, Deutschland hat dabei eine der härtesten Richtlinien überhaupt. Während die Oracle Cloud Services ohnehin schon hohe Standards an Sicherheit und Datenschutz erfüllen, bietet die Oracle in Deutschland deutschen Unternehmen zudem eine nationale Datenspeicherung – eine Anforderung, die das deutsche Datenschutzgesetz für viele Branchen und Anwendungen vorsieht.

Die Nähe zum Internet-Knoten DE-CIX und kurze Latenzzeiten gaben den Ausschlag für Frankfurt am Main. Die neue Installation ist zudem als hochverfügbare Umgebung ausgelegt. Das Backup-Rechenzentrum ist ebenfalls in Deutschland und geht damit konform zum deutschen Datenschutz.

Entscheidend für die Oracle Anwender in Deutschland wird sein, dass auch die Verträge auf dessen Basis Cloud Computing mit Oracle betrieben wird, ebenfalls auf Deutschem Datenschutzrecht basieren und auch für Hochverfügbarkeitsumgebungen eine Spiegelung und Weitergabe der Daten auf Standorte außerhalb Deutschlands vermieden werden.

Ein Blick auf die Datenschutz Anforderungen am Standort Deutschland

Die wichtigsten Anforderungen stammen aus dem Bundesdatenschutzgesetzt (BDSG). Ergänzend gibt es Regelungen in Landesverfassungen und Landesdatenschutzgesetzen. Bei den Definitionen von „Daten“ und deren Schutz spielen „personenbezogene Daten“ immer eine besondere Rolle. Wie weitfassend solche personenbezogenen Daten sein können ist enorm. Selbst IP Adressen können in speziellem Kontext sensible personenbezogene Daten sein.

Die Frage ob und welche Daten überhaupt in der IT verarbeitet werden, hat erst einmal nichts mit Cloud Computing zu tun. Erst bei den Technischen und Organisatorischen Maßnahmen zur Einhaltung des Datenschutzes (TOM) kommen Regelungen zur Beachtung, die beim Cloud Computing anders sind, wie z.B. Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, etc.

Bei der grenzüberschreitenden Datenverarbeitung werden generell nochmal drei verschiedene Gebiete unterschieden:

a) Europäischer Wirtschaftsraum
b) Sichere Drittstaaten
c) Unsichere Drittstaaten

Für Unternehmen, die in solchen Ländern international aktiv sind, kann Cloud Computing erheblich zum Datenschutz beitragen, weil die Mechanismen der Cloud Provider einen höheren Standard haben, als sie selbst im Ausland gewährleisten können.

Im Speziellen runtergebrochen bleiben diese Cloudspezifischen Risiken:

1.) Löschung von Daten:
Unsicherheit bezüglich der vollständigen Löschung von Daten auch bei Verlagerung der Cloud durch den Anbieter

2.) Nachvollziehbarkeit durch Protokollierung
Eine Protokollierung erfolgt zumeist nur beim Anbieter; daraus folgt eine faktische Selbstkontrolle der Anbieter und nicht der verantwortlichen Stelle im Sinne des BDSG

3.) Vervielfältigung und Verteilung
Kaum Gewissheit auf der Anwenderseite, wo auf der Welt Datenverarbeitung stattfindet. Insbesondere kann diese auch fragmentarisch / verteilt geschehen

4.) Unsorgfältige Einführung von Cloud-Lösungen
Durch sehr kurze Bereitstellungszeiträume bedingte Unsorgsamkeit in Bezug auf die datensichere Einrichtung datenverarbeitender Anwendungen

Eine zentrale Eigenschaft des Cloud Computing ist, dass Computerressourcen von den Cloud Anwendern genutzt werden, auf die sie selbst keinen konkreten Zugriff haben. Es ist in der Regel nicht nachvollziehbar, wo und auf welchen Systemen Anwendungen und Daten gespeichert sind, ausgeführt oder verarbeitet werden, besonders dann, wenn der Anbieter des Cloud Computing seine

Dienstleistungen und Services (teilweise) bei anderen Anbietern einkauft und dieses nicht transparent für den Cloud Anwender geschieht

Kontaktadresse:
Stefan Kinnen
Apps Associates GmbH
Flughafenring 11
D-44319 Dortmund

Telefon:	+49 (0) 231-2222 7950
Fax:	+49 (0) 231-2222 7979
E-Mail	stefan.kinnen@appsassociates.com
Internet:	www.appsassociates.com