erst einmal die Hürden der Cloud-spezifischen Konfiguration überwunden sind, lassen sich die von der Oracle-Datenbank bekannten Funktionalitäten nutzen.

Der Initialaufwand war sicher höher, da man erst Erfahrungen mit der Oracle Public Cloud sammeln musste. Dies wird sich bei Folgeprojekten ändern. Insoweit ist die Hybrid-Oracle-Public-Datenbank-Cloud in diesem Fall die sinnvollste Lösung und die Paragon-Data-Oracle-Cloud-Anwendung ist trotz aller verfügbaren Wolken gut sichtbar.

Malthe Griesel
m.griesel@paragon-data.de

Christian Trieb
c.trieb@paragon-data.de

Datenschutz in der Cloud – was wirklich (nicht) geht

Stefan Kinnen, Apps Associates GmbH

Oracle fokussiert viele Lösungen auf Cloud-basierten Ansätzen. Um einen besseren Einstieg in eine Entscheidung pro/contra Cloud aus Sicht des Datenschutzes fällen zu können, zeigt der Artikel einige Aspekte bei der Evaluierung.

Die Gehaltsabrechnung kommt via SaaS aus dem Web und Online-Banking geschieht per Tablet oder Smartphone. Im privaten Bereich ist die Cloud-Nutzung weithin akzeptiert. Marketing- und Personal-Abteilungen im Unternehmen nutzen ebenfalls schon fleißig Cloud Services für bestimmte Projekte. In der IT hingegen ist die Zurückhaltung noch immer groß. Eine Meinung zu Cloud Computing haben viele schnell gefasst. Aber welche gesetzlichen Rahmenbedingungen gelten eigentlich? Was sagt der Datenschutz wirklich? Und was empfehlen die führenden Branchenverbände zur deutschen Cloud-Standortpolitik?

„Cloud-Nutzung wächst – Sicherheitsbedenken bremsen", so fasst die BITKOM basierend auf einer Studie des Wirtschaftsprüfungs- und Beratungsunternehmens KPMG den Cloud-Jahresbericht 2015 zusammen. Im Jahr 2014 ist demnach die Zahl der Cloud-Nutzer in Deutschland weiter gestiegen. Mittlerweile setzt 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 Megatrends wie Big Data und Mobility zukünftig noch stärker herauskristallisieren wird.

Unbegründete Sicherheitsbedenken

Einige Kennzahlen aus der BITKOM-Studie untermauern, dass oft spontan geäußerte Ablehnung gegen Cloud-Angebote mit dem Argument „Datenschutz" nicht unbedingt objektiv begründet werden kann:

- Die Nutzung von Cloud-Diensten wächst weiter. 44 Prozent der Unternehmen in Deutschland setzen bereits Cloud Computing ein – weitere 24 Prozent erwägen es
- 85 Prozent der registrierten IT-Angriffe auf Unternehmen haben nichts mit Cloud Computing zu tun
- 78 Prozent der Private-Cloud-Nutzer bewerten ihre Erfahrungen als positiv
- Nur 8 Prozent der Cloud-Benutzer berichten über Compliance-Vorfälle in Zusammenhang mit der Cloud
- 74 Prozent der Unternehmen versprechen sich von Private-Cloud-Diensten einen verbesserten Zugriff auf IT-Ressourcen und 75 Prozent bestätigen, dass dieses Ziel erreicht wurde

Auffallend ist noch eine andere Zahl: 71 Prozent 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 Prozent der deutschen Cloud-Kunden an ihren Cloud Provider, dass die Rechenzentren in Deutschland betrieben werden (Quelle: BITKOM / KPMG Cloud Monitor 2015).

Die Bedeutung der zwei Oracle-Rechenzentren in Deutschland

Um den Kundenerwartungen gerecht werden zu können, hat Oracle im Februar 2015 in Frankfurt am Main und in München die ersten beiden Cloud-Rechenzentren in Deutschland eröffnet. Mit Frankfurt als Produktions- und München als Backup-Rechenzentrum bietet Oracle nun deutschen Unternehmen eine lokale Cloud-Infrastruktur und erlaubt es Kunden, ihre IT-Aufgaben auch aus der Cloud Datenschutz-konform abzubilden. In den neuen Rechenzentren werden jedoch zunächst nur einige limitierte Produkte aus dem Bereich der Business-Applikationen angeboten. Weitere Cloud Services sollen folgen. Oracle bietet den deutschen Unternehmen eine nationale Datenspeicherung – eine Anforderung, die das deutsche Datenschutzgesetz für viele Branchen und Anwendungen vorsieht. Entscheidend für die Oracle-Anwender in Deutschland wird jedoch sein, dass die Verträge, auf deren 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 nachweislich vermieden wird.

Datenschutz-Anforderungen am Standort Deutschland

Die wichtigsten Anforderungen stammen aus dem Bundesdatenschutzgesetz (BDSG). Ergänzend gibt es Regelungen in Landes-

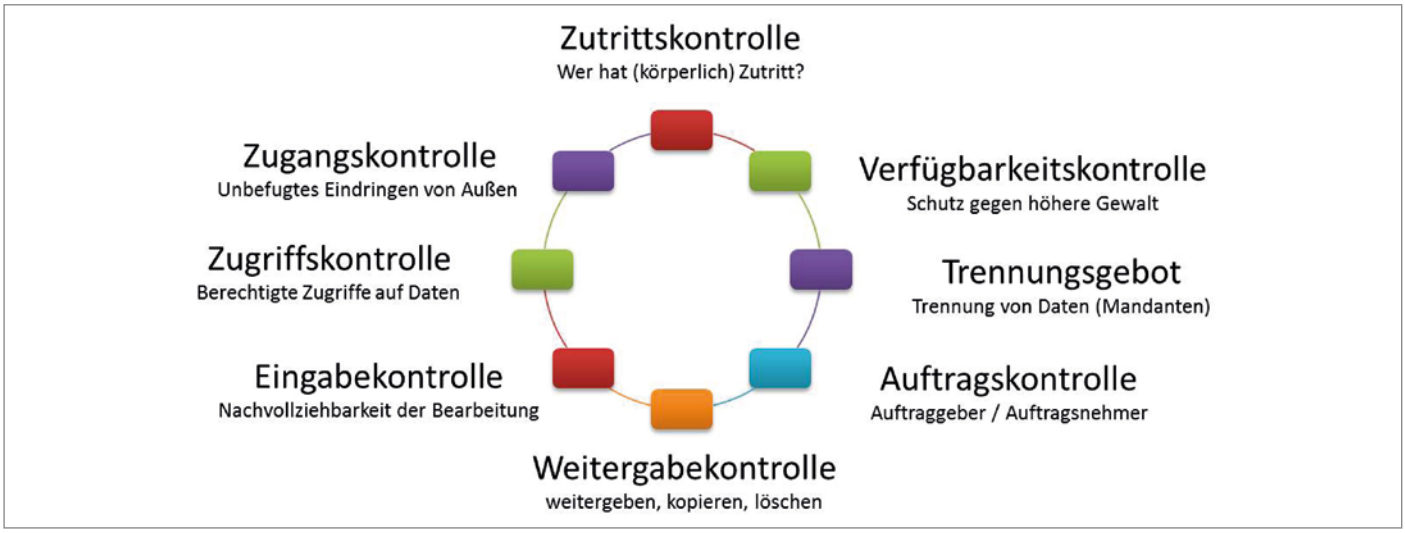

Abbildung 1: Technische und organisatorische Datenschutz-Maßnahmen

verfassungen und Landesdatenschutzgesetzen. Bei den Definitionen von „Daten" und deren Schutz geht es im Wesentlichen um „personenbezogene Daten". Wie weitfassend solche personenbezogenen Daten sein können, ist enorm. Selbst IP-Adressen können in speziellem Kontext sensible personenbezogene Daten sein.

In der Branche werden seit Längerem Forderungen laut, einen einheitlichen europäischen Datenschutz-Standard zu schaffen, der vielen Cloud-Anbietern das Leben leichter machen und auch den Anwendern mehr Vertrauen verschaffen könnte. Die neuesten Tätigkeiten der Bundesregierung deuten darauf hin, dass diese Forderung angekommen ist und auf Verständnis stößt.

Bei der grenzüberschreitenden Datenverarbeitung wird generell zwischen drei Gebieten unterschieden:

- Europäischer Wirtschaftsraum
- Sichere Drittstaaten
- Unsichere Drittstaaten

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

Technische und organisatorische Maßnahmen

Die Frage, ob und welche Daten überhaupt in der IT verarbeitet werden, hat zunächst 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 Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle etc. *(siehe Abbildung 1)*. Im Speziellen heruntergebrochen bleiben diese Cloud-spezifischen Risiken:

- *Löschung von Daten*
  Unsicherheit bezüglich der vollständigen Löschung von Daten auch bei Verlagerung der Cloud durch den Anbieter

- *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

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

- *Unsorgfältige Einführung von Cloud-Lösungen*
  Durch sehr kurze Bereitstellungszeiträume bedingte Achtlosigkeit in Bezug auf die datensichere Einrichtung datenverarbeitender Anwendungen

Eine zentrale Eigenschaft des Cloud Computing ist, dass Computer-Ressourcen 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.

Fazit

Cloud Services pauschal mit dem Argument „Datenschutz" abzulehnen, ist voreilig und längst nicht immer notwendig. Die datenschutzrechtlichen Maßnahmen können auch mit Cloud-Angeboten eingehalten werden. In puncto „IT-Sicherheit" sind Cloud Services manchmal sogar höherwertiger als eigene On-Premise-Installationen. Auf juristischer Ebene sollten sich die Anbieter durch Vereinfachung der Vertragsunterlagen mit klarem Bezug zumindest zu europäischem Recht und die Gesetzgeber ebenfalls durch Vereinfachungen und die Schaffung eines europäischen Standards entgegenkommen.

Stefan Kinnen
stefan.kinnen@appsassociates.com