

Schattenseiten



In den letzten Jahren hat sich im Zuge einer fortschreitenden Virtualisierung von IT-Lösungen ein neues IT-Paradigma entwickelt: Cloud Computing. Gabrielle Schultz sprach mit Prof. Dr. Jan Jürjens, Professor für Software Engineering an der Technischen Universität Dortmund und wissenschaftlicher Koordinator „Enterprise Engineering“ sowie Leiter der Forschungsgruppe „Architekturen für auditable Geschäftsprozess-Ausführungen“ am Fraunhofer ISST, über Potenziale und Sicherheitsrisiken des Cloud Computing.

Im Dezember letzten Jahres konnte bei radio.de mit Sitz in Hamburg und Innsbruck 48 Stunden lang niemand auf die Bürosoftware und auf Daten zugreifen, obwohl die Computer und die Datenleitungen funktionierten. Der Grund war ein Fehler im Bezahlssystem von Google, einem der großen US-Anbieter von Cloud Services. Für mittelständische europäische Kunden ist die Google-Niederlassung in Dublin zuständig, die allerdings niemals telefonisch erreichbar ist. Ist das der Super-GAU für Cloud-Nutzer? Aus Sicht des Cloud-Kunden ist das sicherlich ein Super-GAU. Abhängig davon, um was für einen Kunden es sich handelt, kann man in 48 Stunden auch Pleite gehen. Ich hoffe, dass es den Radiosender noch gibt. Wenn es bei einem Cloud-Angebot keinen leicht erreichbaren Ansprechpartner gibt, kann das im Fall von Problemen in Hinblick auf Zuverlässigkeit und Ausfallsicherheit zu Schwierigkeiten führen. IT-Systeme können allerdings auch ohne Cloud Computing ausfallen. In dem Fall hätte der Radiosender allerdings einen direkten Ansprechpartner gehabt. Vor Ort kann ich notfalls einen Mitarbeiter, der für die IT-Strukturen verantwortlich ist, auch nachts aus dem Bett holen.

Die Idee beim Cloud Computing ist ja, letztendlich Geld zu sparen. Da es aber nichts umsonst gibt, muss ich im Prinzip damit rechnen, dass ich einen schlechteren Service erhalte, wenn ich möglichst viel Geld sparen will. Umgekehrt gibt es aber auch Cloud-Angebote, die bestimmte Service-Standards garantieren (über so genannte „Service Level Agreements“).

Grundsätzlich muss geklärt werden, welcher Teil der Infrastruktur outgesourct werden soll. Wenn es ein Backend-System ist, in dem Daten archiviert werden, dann ist das im Allgemeinen kein Genickbruch, wenn ich vielleicht zwei Tage lang keinen Zugriff habe. Aber wenn das Systeme sind, über die der laufende Betrieb abgewickelt wird, oder Websites im e-commerce-Bereich, über die Produkte verkauft werden, gelten ganz andere Anforderungen an Zuverlässigkeit und Sicherheit.

Ist die Kostenersparnis wirklich so enorm, wenn Unternehmen in der Wolke rechnen lassen?

Prinzipiell kann die Ersparnis enorm sein. Theoretisch lässt sich die mögliche Ersparnis am besten anhand des Prinzips „Follow the sun“ veranschaulichen. Das heißt, die verwendeten IT-Ressourcen werden über die Zeitzonen hinweg verteilt. Klassisches Beispiel sind die Websites, auf denen man TV-Programme ansehen kann. Um 20 Uhr abends in einer gegebenen Zeitzone entsteht ein so genannter Peak, das heißt, zur Prime Time setzen sich Menschen an den Computer und überlegen, was sie im Fernsehen sehen wollen. Das Gleiche passiert in der nächsten Zeitzone, wenn dort 20 Uhr ist. Wenn man jetzt in jeder Zeitzone einen einzelnen Server benötigte, dann würde der, vereinfacht gesagt, 23 Stunden lang nicht viel zu tun haben. Die generelle Idee ist, dass ich nicht 24 Server aufbaue (je einen für jede Zeitzone, der die Webseiten der verschiedenen Anbieter in verschiedenen Ländern enthält), sondern nur einen Server verwende, der in einer Stunde die erste Zeitzone, dann

die nächste und so weiter bedient. Im Extremfall stellt das eine 24-fache Ersparnis dar.

Belegbare Zahlen sind mir allerdings nicht bekannt, aber selbst eine geringe Ersparnis kann relevant sein, die man jedoch in Relation zum möglicherweise reduzierten Service-Level setzen muss.

Derzeit gibt es in der IT-Branche kaum ein öfter benutztes Hype-Wort als Cloud-Computing. IT-Dienste konnten aber schon vor Erfindung dieses Wortes outgesourct werden. Was ist wirklich neu am Cloud Computing?

Der Begriff wird häufig als Marketinginstrument verwendet. Viele Rechenzentren bezeichnen sich per se als Cloud Anbieter, was nicht immer gerechtfertigt ist. Ein wichtiges Ziel beim Cloud Computing ist sicherlich die größere Skalierbarkeit durch Vernetzung einzelner Server-Cluster. Neu ist insbesondere die Idee der globalen Verteilung im Sinne von „Follow the sun“, wie vorhin diskutiert. Es gibt aber auch verschiedene Ebenen des Begriffes Cloud Computing. Ganz unten

38



Prof. Dr. Jan Jürjens: „Die Idee beim Cloud Computing ist ja, letztendlich Geld zu sparen. Da es aber nichts umsonst gibt, kann zu großer Sparwunsch auch zu einem schlechteren Service führen.“



Fotos: Uwe Ernst (www.7-com.net)



in der Hierarchie steht das physikalische System, der Desktop unter dem Schreibtisch, den ich aus einer Cloud heraus mieten kann. Der kann irgendwo auf der Welt stehen. Zur Nutzung brauche ich nur eine Datenleitung. Die nächste Ebene ist das Betriebssystem, das darauf läuft. Neben der Hardware kann ich also auch die Software mieten. In einem weiteren Schritt kann ich Softwareanwendungen wie etwa Bürosoftware mieten. Grundsätzlich lässt sich somit unterscheiden zwischen Infrastructure-as-a-service, Platform-as-a-service und Software-as-a-service. Ich kann aber noch einen Schritt weitergehen, indem ich Business-process-as-a-service miete. Dazu gehören dann beispielsweise die Call Center.

Abgesehen von der Ausfallsicherheit stellt doch auch der Datenschutz ein Problem dar. In den USA gibt es de facto keinen Datenschutz. Würden Sie einem mittelständischen Unternehmen raten, eher einen Cloud Anbieter in Deutschland bzw. in Europa zu vertrauen?

Die Verarbeitung sensibler personenbezogener Daten darf beispielsweise nach dem deutschen Datenschutzgesetz nur in Deutschland erfolgen bzw. innerhalb von Deutschland oder Europa outgesourct werden. In den USA gibt es keine vergleichbar umfassenden gesetzlichen Regelungen zum Datenschutz, die dem europäischen Standard entsprechen würden. Es gibt zwar ein Save Harbor Abkommen zwischen der EU und

bestimmten Anbietern in den USA, das gewährleistet, dass personenbezogene Daten legal in die USA übermittelt werden können. Aber dieses Abkommen wird von den deutschen Gerichten zunehmend kritisch gesehen. Ihre Frage lässt sich aber insgesamt weder pauschal mit ja noch mit nein beantworten, da im Vorfeld sehr genau geklärt werden muss, in welcher Branche das Unternehmen tätig ist und ob die Nutzung eines Cloud-Anbieters in den USA tatsächlich eine konkrete Ersparnis darstellt nach Abwägung aller Aspekte, angefangen bei der Ausfallsicherheit bis hin zum Datenschutz.

Sie leiten am Fraunhofer ISST zwei Projekte, die gerade erst anlaufen und sich mit den Themen Compliance und Security beschäftigen. Was erforschen Sie genau?

In dem Projekt Cloudat werden wir Methoden und Werkzeuge entwickeln, mit denen man die Einhaltung von Sicherheits- und Complianceanforderungen auf der Seite eines Cloud-Anbieters überprüfen kann.

Wenn ein Unternehmen Daten in der Cloud verarbeiten lassen möchte, müssen datenschutzrechtliche Bestimmungen und bestimmte Regularien eingehalten werden. Zum Beispiel müssen bis 2013 alle Versicherungen in Europa Solvency-II-konform handeln. Weiter bestehen Mindestanforderungen an das Risikomanagement (MaRisk VA). Über die Versicherungsbranche

hinaus gibt es ähnliche Richtlinien in anderen Branchen, zum Beispiel für Banken Basel II und MaRisk BA. Einfach ausgedrückt: Schon ohne Cloud ist es schwierig, IT-Risiken, Sicherheitsrisiken, aber auch operationale Risiken unter Einhaltung aller Richtlinien zu managen. Mit Cloud wird es noch schwieriger. Die Softwaretools, die wir hier für den Versicherungsbereich entwickeln, lassen sich auf andere Branchen übertragen.

Bei dem Forschungsprojekt Secure Clouds beschäftigen wir uns mit der Seite der potenziellen Cloudanwender, die beabsichtigen, in die Cloud zu gehen. Welcher Teil der Infrastruktur kann ausgelagert werden? Dürfen Geschäftsprozesse in die Cloud verlagert werden, ohne die Compliance- und Sicherheitsstandards zu verletzen? Die Sicherheit von Cloud Services ist eines der wichtigsten Hindernisse bei der Akzeptanz von Cloud Computing Systemen in Unternehmen. Die Ursache ist zum einen in der mangelnden Anwendung und Unterstützung von Sicherheitstechnik, zum anderen in signifikanten Anforderungen an Skalierbarkeit und Elastizität der Cloud Systeme zu sehen, für die derzeit erst spezielle Sicherheitstechniken entwickelt werden. In unseren Projekten am Fraunhofer ISST versuchen wir, zur Lösung dieser Probleme beizutragen.

Danke für das Gespräch. □

www.isst.fraunhofer.de