

automotiveIT®

Strategien. Produkte. Trends.



Spezial Cloud Computing

Chancen und Risiken

- Die Cloud: Schritt in Richtung Industrialisierung der IT
- Plus: Vereinfachung von Engineering und Distribution
- Minus: Sicherheitsrisiken an Schnittstellen



INTERVIEW

Meike Schäffler. Die IT-Chefin von Benteler über Wachstum und IT



NEUE NETZE

Smart Grid. Wandel in der Energiepolitik. Wie geht es weiter?

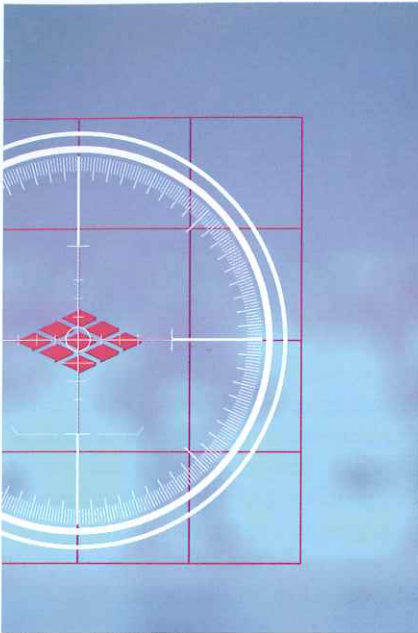


KONZEPTE

Carsharing. Die Rolle der IT in den neuen Mobilitätskonzepten

→ www.automotiveIT.eu

Redundanz in der IT: Viele Unternehmen entrümpeln ihre Softwarelandschaften



SICHERHEITSLAGE

DAS GRÖSSTE HEMMNIS FÜR CLOUD-ANGEBOTE IST DIE ANGST: ANGST VOR DATENDIEBSTAH, VOR KONTROLLVERLUST UND VOR VERSTÖSSEN GEGEN DEN DATENSCHUTZ.

Die Ausgangslage ist klar: „Wenn das bisherige Rechenzentrum mittels Cloud-Technologien und Services flexibilisiert wird, liegen die Herausforderungen vor allem darin, wie SaaS-Lösungen im Unternehmen standardisiert, ausgerollt und in bestehende Geschäftsprozesse integriert werden. Dauerbrenner-Thema ist die Standardisierung von Schnittstellen“, so Oliver Kelkar, Senior Manager beim IT-Dienstleister Mieschke Hofmann und Partner. „Bei isolierten Applikationen mit einem abgeschlossenen Datentopf – wie zum Beispiel im CRM – ist die Verlagerung in die Cloud relativ einfach. Spannender wird es bei der Integration komplexerer Anwendungen“, sagt Gero Decker, Geschäftsführer beim auf Cloud-Anwendungen spezialisierten Softwareanbieter Signavio. „Die ‚Hemdsärmeligkeit‘, mit der Schnittstellen in klassischen Systemen oft geschaffen werden, funktioniert bei Cloud nicht, weil hier die Sicherheit der Schnittstellen beachtet werden muss“, so Decker. Hier komme den Webservices eine wichtige Rolle zu. „Die Schnittstellenfrage muss heute kein Show-Stopper sein. Es gibt viele neue Technologien, mit denen sich

saubere Lösungen finden lassen, wenn man sich dem Thema nicht zu ängstlich nähert“, fasst Decker zusammen.

Die Sicherheitslage in den weiter verbreiteten Private Clouds ist eine deutlich andere als in Public Clouds, wie sie beispielsweise durch Amazon angeboten werden. „Entscheidende Herausforderungen sind hier unter anderem die Übertragungssicherheit, also der Schutz gegen Wirtschaftsspionage und -kriminalität sowie Sabotage, und die Betriebssicherheit, sprich die Verfügbarkeit der Cloud Services“, führt Kelkar aus. Auch die Erfüllung von Compliance-Anforderungen, insbesondere die Nachvollziehbarkeit, sei ein wichtiges Thema. Diese Risiken seien gegen die Chancen abzuwägen. Laut einer Untersuchung der Expertengruppe sind Risikomanagement, Service Level Agreements und Provider Management die wichtigsten Grundlagen für eine profunde Cloud Security. Eine Risikoanalyse für geplante Cloud Services sollte die Betrachtung der Compliance-Problematik einbeziehen. Zudem sollten Arbeitsteilung und Schnittstellen zwischen dem Provider

und dem eigenen Unternehmen geprüft und exakt definiert werden. Das Marktforschungs- und Beratungsunternehmen rät, besonders darauf zu schauen, ob der Cloud-Dienstleister Subunternehmer einsetzt, die zu einer gegebenenfalls negativ veränderten Risikolage führen könnten. Auch die Bedingungen für einen Providerwechsel sollten vorher geklärt werden. Die Einhaltung des Datenschutzgesetzes obliegt dem Unternehmen auch in der Zusammenarbeit mit Cloud-Dienstleistern. Daher muss verbindlich geklärt sein, an welchen Orten die Daten gespeichert werden und ob dort der Datenschutz entsprechend gewährleistet werden kann. Computer Associates (CA) kommt in einer Studie zu dem Schluss, dass Anwendungen wie Identity und Access Management (IAM), die von den IT-Dienstleistern ebenfalls in der Cloud zur Verfügung gestellt werden, für mehr Sicherheit durch Authentifizierung sorgen. Das Jahr 2011 dürfte dem IT-Unternehmen zufolge das Jahr der Cloud-Aktivitäten sein, in dem der Skeptizismus überwunden wird.

Autorin: Daniela Hoffmann