

5 Sicherheit in der Cloud

- Sicherheit in der Cloud ist ein zentrales Thema. Einige einfache Maßnahmen verhelfen bereits zu einer soliden Grundlage.
- Im Vorfeld müssen **die eigenen Anforderungen** an die Sicherheit genau geklärt werden.
- **Es überwiegen die organisatorischen Probleme.** Unter anderem müssen die Mitarbeiter sensibilisiert und geschult werden sowie bestehende und neue Sicherheitskonzepte integriert werden.
- Auf technischer Seite müssen sowohl die Infrastruktur als auch die Daten geschützt werden. Ansätze für ersteres sind bekannt. Der Aspekt der **Datensicherheit** ist zwar teilweise auch bekannt, stellt aber größere Hürden in den Weg, da viele Anbieter nur ein durchschnittliches, aber kein hohes Schutzniveau erbringen.
- **Insgesamt ist die Sicherheit von Cloud-Diensten nicht notwendigerweise schlechter als von Lösungen im eigenen Haus.**

1. Wird die Sicherheit der Cloud-Computing-Lösung in einem **ganzheitlichen** Sicherheitskonzept beurteilt?
2. Hat der Provider eine ausführliche **Analyse der Sicherheitsaspekte** des Cloud-Dienstes durchgeführt, bei der mögliche Schwachstellen und Gegenmaßnahmen analysiert wurden?
3. Durch welche **Zertifikate**, Testate oder externe Überprüfungen kann der Cloud-Anbieter den sicheren Betrieb seiner Services glaubhaft machen und wie kann das Anwenderunternehmen dies überprüfen?
4. Wie wird die **korrekte Funktion** aller Sicherheitsmechanismen gewährleistet und wie wird im Fehlerfall vorgegangen?
5. Sind auch die sicherheitsrelevanten Aspekte der Service-nutzung durch ein **SLA** abgedeckt?
6. Wurde die gesamte Wertschöpfungskette inklusive der Dienstleister des Cloud-Anbieters analysiert?
7. Wie werden die **Kommunikationskanäle** zur Cloud im Sicherheitskonzept berücksichtigt und geschützt?
8. Bieten **alle Rechenzentren** dasselbe Sicherheitsniveau, auch z. B. im Hinblick auf die politische Lage und rechtliche Situation im jeweiligen Land?
9. Ist klar definiert, wer bestimmte sensible Daten einsehen darf und welche **Zugriffskontrollen** sind installiert?
10. Wie erkennt der Cloud-Anbieter, dass ein Dienst **angegriffen** wird?

Das Working Paper No. 3 des Instituts für angewandte Informatik ist eine Studie der **DBIS Group**:



DBIS Group
Prof. Dr. G. Vossen
Institut für Wirtschaftsinformatik
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 3
D-48149 Münster
<http://dbis-group.uni-muenster.de/>

Bitte beachten Sie:

Diese Broschüre gibt lediglich einen **stark verkürzten** Überblick über die wichtigsten Inhalte des Working Paper No. 3 *Database-as-a-Service für kleine und mittlere Unternehmen*.
Wenn Sie Interesse an der vollständigen Studie haben, wenden Sie sich bitte an **Till Haselmann von der DBIS Group** oder das Institut für angewandte Informatik.

Förderkreis der
Angewandten Informatik
an der Westfälischen Wilhelms-
Universität Münster e.V.

Einsteinstraße 62
D-48149 Münster
Tel.: +49 251 83 33797
Fax : +49 251 83 33755



Förderkreis der
Angewandten
Informatik
an der
Westfälischen
Wilhelms-Universität Münster e.V.

Broschüre zum Working Paper No. 3

Database-as-a-Service für kleine und mittlere Unternehmen

Ein Leitfaden für KMU, die „in die
Cloud gehen“ möchten

Till Haselmann
Gottfried Vossen

November 2010

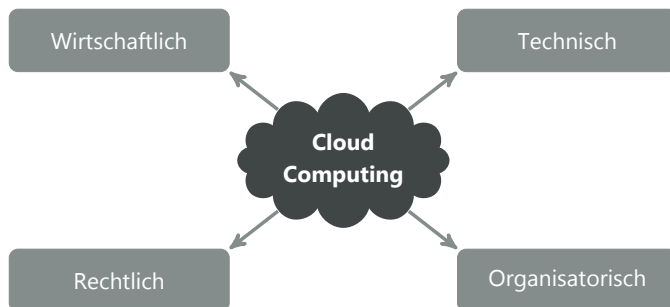
1 Struktur des Berichts



2 Grundlagen Cloud-Computing

In dieser Broschüre werden die wichtigsten Aspekte der jeweiligen Kapitel des Working Paper vorgestellt. Zudem werden zu jedem Abschnitt zehn Leitfragen präsentiert, die einen direkten Einstieg in die praktische Anwendung ermöglichen.

- Cloud-Computing ist keine technische Revolution, aber eine neue Kombination aus Bekanntem und Neuem.
- Es gibt drei Servicemodelle: IaaS, PaaS, SaaS.
- **Database-as-a-Service (DaaS)** bezeichnet eine Klasse von Cloud-Diensten, die Funktionalitäten eines DBS bereitstellen.
- Es gibt vier Arten des Cloud-Betriebs: die öffentliche und nicht-öffentliche Cloud, die Community-Cloud sowie die hybride Cloud.
- Cloud-Computing ist ähnlich dem klassischen IT-Outsourcing, verschiebt aber die Gewichtung der problematischen Aspekte.
- Die Analyse erfolgt entlang von vier Dimensionen:



3 Grundsatzentscheidung

- Cloud-Computing wird in **vier Dimensionen** betrachtet.
- **Wirtschaftlich** kann Cloud-Computing sehr attraktiv sein, muss es aber nicht, insbesondere bei individuellen Verträgen.
- **Technisch** birgt Cloud-Computing für den Anwender nur wenig wirklich neue Herausforderungen, fordert aber oft eine Anpassung bestehender Systeme.
- **Rechtlich** ist Cloud-Computing noch höchst problematisch und derzeit weitgehend ungeklärt.
- **Organisatorisch** erfordert Cloud-Computing stringente Abläufe, die gegebenenfalls im Unternehmen erst noch einzuführen sind.
- Die Entwicklung einer **Cloud-Strategie** auf Managementebene ist eine essentielle Voraussetzung für jedes Cloud-Projekt.

1. Gibt es **grundsätzliche Vorbehalte**, das System auszulagern, bzw. wäre ein klassisches Outsourcing des Systems denkbar?
2. Was genau soll ausgelagert werden und durch welche Art von Cloud-Ressourcen soll die Auslagerung realisiert werden?
3. Handelt es sich bei der auszulagernden Funktionalität um eine, die das **Kerngeschäft** des Unternehmens direkt betrifft?
4. Welche speziellen **rechtlichen Rahmenbedingungen** müssen beim Auslagern des Systems eingehalten werden?
5. Benötigt die Anwendung eher einen **intensiven Datenaustausch** zwischen Cloud und Unternehmen oder funktioniert sie eher isoliert? In anderen Worten: Befinden sich Daten und Logik am selben Ort?
6. Wie ist die **Last des Systems** zu charakterisieren? Gibt es nennenswerte regelmäßige oder unvorhersehbare Schwankungen? Wie ist das Verhältnis von Lastspitzen zur durchschnittlichen Last?
7. Profitiert die Anwendung von **Elastizität**, d. h., ist sie (bevorzugt horizontal) skalierbar?
8. Soll ein bestehendes System ausgelagert und durch einen Cloud-Dienst ersetzt werden oder soll neue Funktionalität durch die Cloud bereitgestellt werden? Müsste im letzteren Fall für die Einführung im eigenen Unternehmen neue Hardware oder Software angeschafft werden?
9. Hat das System eine beschränkte **Lebensdauer**, z. B. durch ein klar definiertes Projektende?
10. Gibt es bereits **Präzedenzfälle** am Markt, in denen Unternehmen in vergleichbarer Situation ähnliche Lösungen realisiert haben?

4 Auswahl des Cloud-Providers

- Bei der Auswahl des Anbieters müssen alle vier Dimensionen des Cloud-Computings betrachtet werden.
- **Wirtschaftlich** spielen die Reputation des Anbieters, sein Preismodell und die zu erwartenden Lock-in-Effekte die wichtigste Rolle.
- **Technisch** muss vor allem auf die Datensicherung, die Leistungsfähigkeit der Cloud und die Integration in bestehende Anwendungen geachtet werden.
- **Rechtlich** ist zu klären, ob der Anbieter alle relevanten Regularien erfüllt. Ebenfalls zu klären sind Ausstiegsszenarien und z. B. Preisänderungen während der Vertragslaufzeit.
- **Organisatorisch** ist ein strukturiertes Vorgehen zur Anbieterauswahl inklusive Dokumentation gefordert. Wichtige Aspekte dieser Dimension sind die Support-Leistungen und die Kommunikation mit dem Anbieter.

1. Wie etabliert, groß und zuverlässig ist der Cloud-Anbieter nach eigener **Meinung** und nach Meinung seiner (un-)zufriedenen Kunden? Kann der Cloud-Anbieter dies durch relevante **Zertifizierungen** z. B. nach SAS 70 oder ISO/IEC 27001 belegen?
2. Wie viel **Kontrolle** kann das Unternehmen über den Cloud-Anbieter ausüben? Wie können die tatsächliche Umsetzung der versprochenen Maßnahmen und Leistungen vor Ort überprüft werden?
3. Ist und bleibt das Anwenderunternehmen **alleiniger Eigentümer** seiner Daten?
4. Wo und in welchen **Rechenzentren** werden die Daten durch den Anbieter verarbeitet?
5. In welchem Ausmaß muss das Anwenderunternehmen seine **Prozesse und Systeme anpassen**, um sinnvoll mit dem Anbieter zusammenarbeiten zu können?
6. Erfüllt der Cloud-Service alle notwendigen **gesetzlichen Vorschriften**? Wird insbesondere das BDSG vollständig umgesetzt?
7. Wie umfangreich, flexibel und praxistauglich sind die Möglichkeiten, **individuelle SLAs** zu vereinbaren?
8. Wie umfangreich ist die implementierte **Backupstrategie** und wie flexibel können Daten wiederhergestellt werden?
9. Sind die **Support-Leistungen** des Anbieters für die Bedürfnisse des Cloud-Nutzers angemessen?
10. Wie überprüft der Anbieter seine Mitarbeiter bzw. Dienstleister vor der Einstellung bzw. Auftragsvergabe?