Prüfen Sie Cloud-Angebote mit Weitblick

Cloud – auf ein W.O.R.T.

Ein Umzug in die Cloud verspricht Flexibilität und Sparpotenzial. Das Ganze hat aber auch eine Kehrseite: So verursacht etwa eine höhere Sicherheit höhere Kosten. Daher ist eine umfassende Betrachtung nötig, um eine Cloud beurteilen zu können, auch als DSB – eine Betrachtung auf ein W.O.R.T eben, die wirtschaftliche (W.), organisatorische (O.), rechtliche (R.) und technische (T.) Aspekte berücksichtigt.

Wirtschaftliche Aspekte

Die Betrachtung der Wirtschaftlichkeit ist für eine Entscheidungsfindung pro oder contra Cloud von zentraler Bedeutung.

Zu einer realistischen Einschätzung gehört, nicht nur die Vorteile zu sehen, sondern z.B. auch die Kosten eines möglichen Anbieterwechsels oder die einer Rückführung ins eigene Unternehmen einzubeziehen. Ebenso schlagen IT-Sicherheit und Datenschutz nicht unerheblich zu Buche.

Organisatorische Notwendigkeiten …

Die organisatorischen Aspekte beim Umstieg auf Cloud Computing betreffen vor allem drei Bereiche:

1. die eigene IT-Abteilung
2. die Datenformate und die Schnittstellen
3. die Vertragsabwicklung

1. … für die eigene IT-Abteilung

Es wäre ein Irrtum, zu meinen, mit dem Transfer der Anwendungen in die Cloud hätte sich das Thema „Eigenbetrieb der IT“ erledigt. Server und Applikationen mögen in die Wolke transferiert sein. Trotzdem werden Clients und das interne Netz im Unternehmen verbleiben – und sie müssen auch dort betreut werden.

Für den Notfall muss vorgesorgt sein

Außerdem kann ein Unternehmen aus den verschiedensten Gründen gezwungen sein, in einem relativ kurzen Zeitraum einen Transfer seiner Daten zu einem anderen Cloud-Anbieter oder in das eigene Unternehmen zurück vorzunehmen.

Was Cloud Computing auf der einen Seite einspart, kann auf der anderen Seite erhebliche Kosten verursachen

Sind dann im Vorfeld keine Vorkehrungen für solche Notfälle getroffen worden, steht ein Unternehmen vor zwei großen Problemen, die es innerhalb kürzester Zeit lösen muss:

- Bei einem Wechsel in das eigene Unternehmen muss binnen kurzer Zeit entsprechende Hardware zur Verfügung stehen.
- Bei den Mitarbeitern der IT-Abteilung hat ein Verlust an Kenntnissen eingesetzt, der sich verstärkt, je länger und je mehr Abläufe über die Cloud abgewickelt werden. Schon diese Tatsache allein kann dazu führen, dass eine erneute Migration mit erheblichen Schwierigkeiten verbunden und so ein Anbieterwechsel nur noch zu immens hohen Kosten möglich ist.

2. … für Formate und Schnittstellen

Vor einer Migration müssen Kunden und Anbieter Schnittstellen und Datenformate anpassen.

Offene Schnittstellen könnten die Portabilität zwischen den einzelnen Anbietern fördern. Einheitliche und offene Schnittstellen und Datenformate sind bisher aber eine Ausnahme. Sie würden der Sicherung des Geschäftsmodells einzelner Anbieter geradezu entgegenstehen.

Für eine komplikationslose Migration zu einem anderen Anbieter oder die Rückführung der Datenverarbeitung in die eigene Umgebung ist zusätzlich noch eine Übereinstimmung der Applikationslogik und des Datenmodells zwischen altem und neuem Anbieter erforderlich.

Gefahr: Effizienzverlust durch Anpassung an den Cloud-Anbieter

Durch die anbieterseitige Standardisierung kann es notwendig werden, die eigenen Prozesse mit dem damit verbundenen Aufwand anzupassen.

Damit stellt sich die Frage, ob sich die geschäftlichen Kernprozesse intern dann noch genauso effizient erbringen lassen wie zuvor beim Einsatz interner IT-Verfahren.

3. … im Rahmen der Vertragsabwicklung: Wie den Anbieter angemessen kontrollieren?

Wichtig für eine ordentliche Vertragsabwicklung sind die Kontrollmöglichkeiten des Auftraggebers.

Verfügbarkeit und Systemleistung der jeweiligen Cloud sind noch relativ leicht zu überprüfen. Schwieriger ist es bei den „security logs“. Selbst wenn die notwendigen Kenntnisse zur Interpretation dieser Protokolle vorhanden

sind, hat der Auftraggeber oft keinen direkten Zugriff darauf.

Dadurch ist klar, dass die propagierten Konventionalstrafen der Verträge häufig ins Leere laufen: Der Auftraggeber erhält von aufgetretenen Abweichungen nämlich keine Kenntnis oder ist technisch-organisatorisch nicht in der Lage, die Protokolle in adäquater Weise zu interpretieren.

Die wichtigsten rechtlichen Fragen

Die Fragen der rechtlichen Zulässigkeit der Verarbeitung von personenbezogenen Daten in der Cloud werden kontrovers diskutiert. Diese Diskussion soll hier nicht aufgenommen, sondern lediglich einige eher praktische Aspekte aufgeführt werden.

Cloud-Zertifikate stecken derzeit noch in den Kinderschuhen

Der Auftraggeber hat die Pflicht, sich von dem Willen und der Fähigkeit des Auftragnehmers zu überzeugen, die vereinbarten Leistungen und gesetzlichen Forderungen, z.B. im Datenschutz, auch tatsächlich zu erbringen.

Eine Hilfe könnten hier etablierte Zertifikate darstellen. Sie sind aber erst in der Entwicklung, und so lassen sich über die Qualität eines Cloud-Anbieters bisher nur wenig verlässliche Aussagen machen. Zertifikate bieten zudem lediglich eine Orientierungshilfe; die rechtlichen Pflichten verbleiben im Kern beim Auftraggeber.

Ein Gerichtsstand im Ausland kann teuer werden

Eine ganz andere Herausforderung kann die rechtliche Durchsetzung von vereinbarten Konventionalstrafen oder auch von Schadenersatzansprüchen gegenüber dem Anbieter dann sein, wenn sich der Gerichtsstand im Ausland befindet.

Was einem großen Konzern noch möglich wäre, kann für den kleinen Mittelständler zur wirtschaftlichen Bedrohung werden.

Technische Anforderungen: Wie steht es z.B. um eine zuverlässige und geschützte Internetanbindung?

Die Frage einer zuverlässigen und geschützten Internetanbindung hat zentrale Bedeutung. Denn eine Störung der Netzanbindung kann gleichbedeutend mit einer Nichtverfügbarkeit und Produktivitätseinschränkung sein. Gegebenenfalls muss das Unternehmen daher Sorge für eine redundante Netzanbindung tragen.

Zudem kann eine Offline-Nutzung mit Synchronisationsmechanismen erforderlich werden, um die Produktivitätsausfälle annähernd zu kompensieren.

Wirtschaftsspionage per Verschlüsselung ausschließen

Die Wahrung der Vertraulichkeit von Daten in der Cloud sollte ebenfalls gewährleistet sein. Gerade für technologieorientierte Unternehmen ist das Thema Wirtschaftsspionage nicht von der Hand zu weisen – und die Cloud wird als Sammelbecken von Informationen sicherlich jeden professionellen Ausspäher magisch anziehen.

Spätestens jetzt stellt sich die Frage nach einer zuverlässigen Verschlüsselung der Geschäftsgeheimnisse. Soll eine sichere Verschlüsselung realisiert werden, ist auch die Frage zu klären, ob die gewünschten Cloud-Applikationen eine verschlüsselte Verarbeitung unterstützen.

Auf ewig verschlüsselt?

In den meisten Fällen wird dazu ein erheblicher Aufwand notwendig sein. Ein Schlüsselmanagement wird zwingend. Achtung: Nicht mehr zu entschlüsselnde Daten kommen dem unwiederbringlichen Löschen gleich!

Fazit: Keine Hektik!

Würde man den Anbietern Glauben schenken, befindet sich fast jeder in der Cloud, nur man selbst noch nicht. Dass diese Sicht nicht zwingend ist, zeigt die bisherige Marktentwicklung. Es besteht kein Grund zur Hektik.

Ihr Unternehmen sollte sich zusammen mit Ihnen als Datenschutzbeauftragtem ausreichend Zeit für eine besonnene Bewertung der Chancen und Risiken unter Berücksichtigung der Lebenszyklen nehmen. Sie sollten im Interesse des Unternehmens und des Datenschutzes im Vordergrund stehen. Dabei sind die ständige Marktbeobachtung und eine Bewertung der Entwicklung der Produktreife einer Cloud ein weiteres Muss.

Dr. Stefan Reuschke

Aufsichtsratsvorsitzender der Grid e.G., eines Kompetenznetzwerks für Datenschutz.

Unabhängigkeit kostet!

Viele der angenommenen wirtschaftlichen Vorteile des Cloud Computing reduzieren sich bei genauer Betrachtung erheblich, zumindest dann, wenn ein Unternehmen nicht gänzlich abhängig von einem Cloud-Anbieter sein und die Fähigkeit behalten will, den Anbieter zu wechseln. In Fragen der Anbindung an das Netz und vor allem bei der Sicherung der Vertraulichkeit der übertragenen Daten entstehen durch die Nutzung der Cloud Zusatzkosten.

Das Argument „übertriebenes Sicherheitsdenken“ zieht nicht

Diese Zusatzkosten entstehen nicht etwa aus übertriebenem Sicherheitsdenken, sondern sind Schlüsse aus ganz normalen Anforderungen an die Sicherheit und Zuverlässigkeit der IT-Anwendungen. Als Maßstab lassen sich die bisher gestellten Anforderungen an die eigene IT verwenden. Nur unter der Berücksichtigung dieser Kosten ist eine wirklich faire Abwägung möglich!