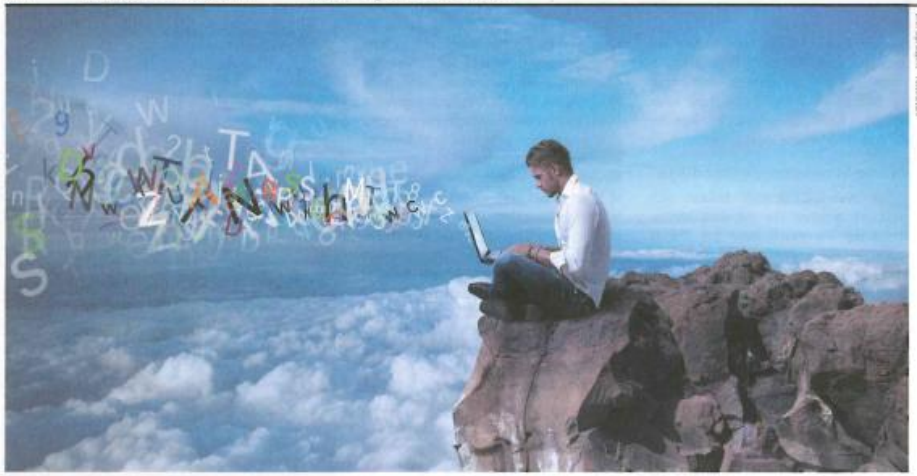

Bild: dpa/picture-alliance

Mehr Überblick im globalen Durcheinander

Cloud-Computing ist bereits seit Jahren das beherrschende Thema der ITK-Branche, obwohl es immer noch an internationalen einheitlichen Standards mangelt. Definierte Mindestanforderungen helfen Unternehmen, den Überblick zu behalten und trotz Wildwuchs an Normen, Richtlinien und Begriffen Cloud-Produkte richtig einzuschätzen.

Global betrachtet herrscht in Sachen Cloud-Computing und Standardisierung nach wie vor keine Einheitlichkeit. Internationale und nationale Bestimmungen weichen voneinander ab oder stehen sich gegenseitig im Weg. Sogar Fachtermini sind zum Teil unterschiedlich belegt und stiften Verwirrung. Auch auf technischer Ebene liegt kein einheitliches Niveau vor. Verschiedene Institutionen, wie zum Beispiel für Deutschland das Bundesinstitut für Sicherheit in der Informationstechnik BSI oder auf internationaler Ebene das Europäische Institut für Telekommunikation sowie die Eurocloud, versuchen seit Jahren, Ordnung ins Richtlinien-Chaos zu bringen und Einfluss auf die Entwicklung zu nehmen – mit ganz unterschiedlichen Erfolgen.

Dabei sind einheitliche Standards besonders im Hinblick auf die Globalisierung extrem wichtig. Sie sind nicht nur für potenzielle Nutzer, die über die Landesgrenzen hinweg agieren, unverzichtbare Orientierungs- und Entscheidungshilfen, sondern auch für kleine regionale Unternehmen. Hier sind vor allem Interoperabilität, Datenschutz und Compliance-Anforderungen entscheidende Faktoren.

Der Stand der Dinge im Detail

Die Standardisierung befindet sich allerdings auf ganz unterschiedlichen Niveaus. Derzeit gibt es laut BMWI einige große Trends, die Entwicklungen in der Wolke wesentlich beeinflussen werden. Die staatliche Mitwirkung gestaltet sich in den großen Industrie-Nationen nach wie vor sehr unterschiedlich. Vor allem die USA nehmen hier eine Vorreiterrolle ein. Beispielsweise mit der „NIST-Roadmap" oder dem „Cloud first"-Grundsatz: Er verpflichtet alle US-Behörden bei IT-Investitionsentscheidungen immer zuerst eine Cloud-Variante zu evaluieren. Europa ist in dieser Hinsicht längst nicht so weit, allerdings gibt es hier verschiedene staatlich getriebene F&E-Projekte, die die Standardisierung vorantreiben sollen. In Deutschland gehört beispielsweise die Trusted-Cloud-Initiative dazu.

Auch wenn Cloud-Anbieter insgesamt einen überaus hohen Automatisierungsgrad anstreben, sind sie von wirklich aussagekräftigen Standardisierungen noch weit entfernt. Seit 2009 gibt es erste, allerdings bisher eher unvollkommene Versuche, Cloud-Zertifikate einzuführen. Dazu gehören beispielsweise die Euro-Cloud-Initiative, Trusted-in-Cloud oder das Cloud-Audit. Wirklich durchgesetzt hat sich bisher allerdings keines dieser Zertifikate. Wie in anderen Geschäftsbereichen auch, versuchen Hersteller und Anbieter das Vertrauen in die Cloud zu stärken. Dazu gehören etwa SAP mit dem „SAP Certified Provider of Cloud Services" oder Cisco Systems mit dem „Cloud and Managed Services Master".

Zu begrüßen ist die zunehmende Einbeziehung vorhandener Standards und Systeme wie ITIL oder Cobit. Gerade in einer prozessgesteuerten IT werden Standards zur Definition und Adressierung komplexer Anforderungen benötigt.

Einen dritten Trend im Zuge der Standardisierungsbemühungen treiben die Nachzügler des Cloud-Marktes voran: Sie setzen vor allem auf offene Standards. Welchen Gesetzen sich diese offenen Standards allerdings unterwerfen, ist von Anbieter zu Anbieter häufig unterschiedlich. Frei nach dem Motto „Anything goes" sind hier vor allem individualisierte Services zu finden, die nur eingeschränkt automatisierbar sind. Hersteller und Anbieter offener Standards haben sich zu Initiativen wie DMTF Open Cloud Standards Incubator oder Open Cloud Consortium zusammengeschlossen.

Auffällig ist, dass die meisten bisherigen Cloud-Lösungen keine Konformität mit geltendem deutschem oder europäischem Recht garantieren. Das heißt für die Vertragsnehmer, dass sie sich im Vorfeld en Detail absichern müssen. Im Einzelfall kann das einen hohen Aufwand bedeuten, denn die Anzahl relevanter Rechtsgebiete ist sehr umfangreich. So zählen Datenschutz, Sicherheitsrecht, Strafprozessrecht, Verbraucherrecht oder IT-Vertragsrecht. Ohne eine detailgenaue Prüfung von fachkundigen Anwälten bestehen also erhebliche Haftungsrisiken. Verbindliche, staatlich gestützte Standards würden hier zu erheblich mehr Rechtssicherheit beitragen.

Knackpunkt Datenschutz

Ein großes Thema der Standardisierungsbemühungen ist auch der Datenschutz. Er ist ein wichtiger Indikator für die Qualität von Cloud-Services. Die im internationalen Vergleich strengen deutschen Vorschriften zum Thema Datenschutz machen hiesige Cloud-Provider aus internationaler Sicht besonders interessant. Da sich die Standards in Deutschland in der Regel auf sehr hohem Niveau befinden, versprechen sich national wie international agierende Kunden größtmögliche Sicherheiten und Transparenz auf allen Ebenen.

Der Schutz der Daten auf Servern innerhalb Deutschlands ist im Bundesdatenschutzgesetz sichergestellt. Zusätzlich beschäftigt sich der Düsseldorfer Kreis, als oberste Datenschutzbehörde, mit allen Aspekten des Datenschutzes im nicht-öffentlichen Bereich. Daneben existieren in Deutschland verschiedene, vom Staat unabhängige Kontrollinstanzen und Institutionen. Im Gegensatz zu anderen Ländern zählt die Rechtslage hierzulande zu den sichersten der Welt und reguliert vor allem auch den Zugriff des Staates auf die gespeicherten Daten.

Flucht vor staatlichem Zugriff

Staatliche Kontrolle und Zugriff sind sensible Punkte, die deutsche Cloud-Provider für ausländische Unternehmen so interessant machen. Deutsche Behörden benötigen schwerwiegende und überzeugende Beweise für Rechtsverstöße sowie einen richterlichen Beschluss, um Zugriff auf die Server deutscher Provider zu erhalten. Andere Länder wie die USA, Russland oder China handhaben den staatlichen Zugriff deutlich laxer. Mit dem Erlass des Patriot-Acts im Jahr 2001 erhielten die US-amerikanischen Behörden gewissermaßen einen Freibrief für Zugriff auf Daten, auch ohne Indizien für eine Straftat. Er erlaubt zusätzlich, die Server von US-Tochterfirmen mit Sitz im Ausland zu durchsuchen. Zudem gibt es in den USA keine unabhängigen Instanzen zur Datenschutzkontrolle. In China hingegen liegt alles in den Händen der staatlichen Regulierung. Das Internet ist dort abgeschottet und unterliegt der Zensur. Auf die chinesischen Netze haben nicht-staatliche Organisationen dagegen nur eingeschränkten Einfluss. Ständig wiederkehrende Verdachtsmomente zur Spionage von sensiblen Geschäftsdaten wecken bei den Unternehmen kein Vertrauen. In Russland ist die Situation noch nicht so verschärft wie in China, doch bewegt sich das Land nach Einschätzung vieler Experten auf diese Verhältnisse zu. Die Regierung setzt sich verstärkt für Zensur sowie strenge staatliche Regulierung und Einflussnahme ein. Immer wieder gibt es Meldungen über lapidare Beweggründe seitens russischer Behörden, um auf Daten zuzugreifen.

„Made in Germany" sehr gefragt

„Made in Germany" könnte also auch in Sachen Cloud-Computing künftig zum Exportschlager werden. Das Prädikat, das vor über 200 Jahren ursprünglich als Warnung vor Nachahmern britischer Qualitätsprodukte eingeführt wurde, steht heute als Qualitäts- und Gütesiegel in internationaler Wertschätzung. Menschen rund um den Globus verbinden kein anderes Ländersiegel so eng mit Fachkenntnis, Zuverlässigkeit und Qualität. Von dieser hohen Wertschätzung profitieren deutsche Firmen über Ländergrenzen hinaus. Für Cloud-Provider in Deutschland ist ihr Standort also ein entscheidender, internationaler Wettbewerbsvorteil. „Made in Germany" beinhaltet aber nicht nur ein hohes Datenschutzniveau aufgrund der deutschen Gesetzgebung. Das Gütesiegel bezieht auch Servicequalität und Sicherheit in das Versprechen mit ein. Es steht für die außerordentlichen Ansprüche, die Provider hierzulande an sich stellen. Im internationalen Vergleich arbeiten sie mit hohen, transparenten Standards. *(CR)*

Cloud-Checkliste

Worauf sich Unternehmen verlassen können sollten

- **Datenschutz** – gewährleisteter Schutz personenbezogener Daten nach BDSG
- **Compliance** – alle technischen Voraussetzungen zur Einhaltung rechtlicher Bestimmungen müssen erfüllt sein
- **Location-Check** – klares Offenlegen, an welchen Standorten die Daten gespeichert sind und wie dort der Zugriff durch Dritte geregelt ist
- **Transparenz** – Information über staatliche Eingriffs- und Einsichtsrechte sowie über gerichtlich festlegbare Einsichtsrechte Dritter an internationalen Standorten
- **Hohe Prozesssicherheit** – Betrieb nach definierten Prozessrahmen wie ITIL oder Cobit
- **IT-Sicherheit** – durchgängige, mandantenfähige Sicherheitsarchitektur auf allen Ebenen (Rechenzentrum, Netz, Plattform, Anwendungen)
- **SLAs** – Sicherstellen aussagekräftiger und eindeutiger SLAs, Definition der Rahmenbedingungen zu deren Gültigkeit
- **Risikominimierung** – Sicherstellung des Betriebs bei Insolvenz etc.
- **Vendor-Lock-in** – Klare Richtlinien für die Daten- und Service-Übergabe am Ende der Vertragslaufzeit
- **Zertifikate** – Transparenz durch international anerkannte Zertifizierungen wie ISO 27001 und 9001
- **Interoperabilität** – standardisierte oder offene Schnittstellen zur reibungslosen Zusammenarbeit zwischen Diensten *(CR)*

Josef Glöckl-Frohnholzer,
Geschäftsführer bei BCC