Helmut Reimer, Christoph Wegener

IT Compliance und Governance: Cloud Computing erweitert den Horizont

Cloud Computing ist erst seit wenigen Jahren der zusammenfassende Begriff für IT-Prozesse mit verteilten Ressourcen. In großen Unternehmen haben sich dafür die Vorstufen in einem langen Zeitraum herausgebildet. Die Etappen Rechenzentren mit Stapelverarbeitung, Zentralrechner mit Arbeitsplatzterminals, autonome und dann vernetzte Arbeitsplatzrechner sind uns allen geläufig. Die letztgenannte Stufe der Entwicklung führte zu enorm steigenden IT-Managementanforderungen und Aufwänden. Serverparks in den Unternehmen sind das Ergebnis.

Parallel zur technologischen Entwicklung sind inzwischen fast alle Unternehmensabläufe vollständig von der Verfügbarkeit der IT-Unterstützung abhängig geworden. Infolgedessen müssen auch die IT-Ressourcen heute streng wirtschaftlich und rechtlich gebotenen Vorschriften folgen. Zu diesem Zweck ist ein ganzes Spektrum von Standards und Werkzeugen für die Erfüllung gesetzlicher Vorgaben (IT Compliance) entwickelt worden. Hierbei geht es vor allem um die Qualitäten der IT-Prozesse in Bezug auf Stabilität, Steuerbarkeit, Datensicherheit und Datenschutz.

Da die Vorstände oder Geschäftsführer der Unternehmen für Schäden durch die Verletzung von Vorschriften oder eine ungenügende Compliance haften, sind Organisation, Steuerung und Kontrolle der IT und der IT-Prozesse eines Unternehmens Aufgaben der Unternehmensführung. Diese IT Governance dient der Ausrichtung der IT-Prozesse an der Unternehmensstrategie und steht in enger Verbindung zum ganzheitlichen Corporate Governance-Ansatz. Sie schließt ausdrücklich eine angemessene Strategie zum Umgang mit den unvermeidlichen Risiken ein.

Das über einige Jahre hochgelobte Outsourcing von IT-Leistungen und IT-Services war ein Praxisfeld, das die Entwicklung weiterer methodischer Elemente für Compliance und Governance erforderte. Beispielhaft seien hier die Service Level Agreements (SLA) genannt. Diese werden häufig insbesondere zur Regelung der Verfügbarkeit einer Dienstleistung oder als spezielles Security SLA zur vertraglichen Regelung der Informationssicherheit eingesetzt. Es hat sich allerdings in der Folge gezeigt, dass sowohl hinsichtlich der erwarteten Ökonomie als auch bei der Steuerung des Risikos mehr Nachteile als Vorteile entstanden.

Cloud Computing kann damit prinzipiell auf einem soliden methodischen Fundament und entsprechenden Erfahrungen im Umgang mit verteilten IT-Ressourcen aufbauen. Gleichzeitig beinhaltet diese neue begriffliche Zusammenfassung zukünftiger IT-Strukturen die Vision, mit den früher erkannten Risiken für Daten, Identitäten und Infrastrukturen wirtschaftlicher und sicherer umgehen zu können.

Dabei sind neue Ansätze zu verfolgen, um die Vorgaben im Bereich Compliance und Governance mit Ausrichtung an den wirtschaftlichen Zielen angemessen umsetzen zu können. Die Cloud-Idee treibt hier die Weiterentwicklung von Standards für die IT-Sicherheit und das Sicherheitsmanagement voran. Neben der Möglichkeit, auf dieser Grundlage sichere, flexible und stabile Cloud-Services anbieten zu können, entstehen dabei aber auch Vorteile für die traditionelle IT: Uneinheitliche Strukturen und damit verbundene kostenintensive Konstellationen gehören endgültig der Vergangenheit an, Prozesse werden damit erheblich vereinfacht.

Über diese Standardisierungsansätze hinaus ebnet die Cloud aber auch andere Wege zu mehr Informationssicherheit. So schafft sie aufgrund ihrer strukturellen Eigenschaften eine prinzipiell mögliche Ausfallsicherheit. Aber auch ein anderer Aspekt, der oftmals intuitiv als negativ betrachtet wird, ist hier von Relevanz: Der Wegfall der Perimeter-Firewalls. Auf den ersten Blick erzeugt die Vorstellung, beim Nutzer von Cloud Computing keine zentrale Firewall mehr betreiben zu können, enorme Unsicherheit. Konsequent weiter gedacht führt er aber zu einem notwendigerweise verbesserten Schutz aller Endgeräte und damit zu einem deutlich verbesserten Sicherheitsniveau. Ob diese Konzepte in Zukunft nur teilweise oder wirklich vollständig umgesetzt werden können, ist und bleibt eine spannende Frage.

Möglicherweise sind Private Clouds – in konsequenter Fortsetzung der Entwicklung aktueller IT-Strukturen – als Übergangslösung ein erster Ansatz. Werden diese gar vom Unternehmen selbst betrieben, schaffen sie genau die Standardisierung und das Perimeter, das in der Cloud bisher noch so schmerzlich vermisst wird. Dieser Weg schöpft das Cloud Computing Potential natürlich nicht wirklich aus, kann aber weitere Entwicklungen hin zur Akzeptanz von echten (Public) Clouds mit der dann verfügbaren Flexibilität und Skalierbarkeit unterstützen.

Eine Hürde, die dem Compliance- bzw. Governance-Manager im Hinblick auf das Cloud Computing das Leben erschwert, ist die Tatsache, dass es sich bei einer Cloud prinzipiell um ein internationales, länderübergreifendes Konstrukt handelt, damit sind aber dann auch vielfältige, länderspezifische Regelungen einzuhalten. Dies gilt sowohl in Bezug auf externe Regelungen, etwa gesetzliche Vorgaben, aber auch für interne Regularien, die in unterschiedlichen Ländern ebenfalls eine andere Perspektive bekommen können. Letzteres ist ein Umstand, den alle international agierende Unternehmen bereits auch ohne Cloud Computing mehr oder weniger schmerzhaft erfahren mussten.

Bleibt festzuhalten, dass Cloud Computing trotz oder gerade wegen der noch bestehenden Probleme als Schlüssel zum Erfolg gesehen werden kann. Denn obwohl viele Fragen zum Cloud Computing noch nicht beantwortet sind: Letztendlich bietet die konsequente Umsetzung des Cloud-Ansatzes eine Chance für mehr Informationssicherheit, und das sogar, ohne die Cloud tatsächlich nutzen zu müssen.