



Link: <https://www.cio.de/a/compliance-im-cloud-zeitalter,3102579>

Neue Herausforderungen

Compliance im Cloud-Zeitalter

Datum: 29.01.2015

Autor(en): Klaus Manhart

Cloud Computing bedeutet nicht nur Flexibilität und Kostenersparnis. Es bringt auch neue Herausforderungen für CIOs und Sicherheitsexperten. Vor allem das Risiko von Compliance-Verletzungen nimmt mit der Verbreitung von Cloud-Services deutlich zu. Für IT-Verantwortliche gilt es, darauf zu achten, dass Datenschutzbestimmungen und Compliance-Vorgaben lückenlos erfüllt werden.

Was bedeutet die wachsende Verbreitung von Cloud Computing für die IT-Sicherheit und Compliance-Maßnahmen? Die Flexibilität, die man beim Cloud Computing gewinnt, erhöht gleichzeitig das Risiko von Compliance-Verletzungen - wie den Verlust unternehmenskritischer Daten. In der Cloud ist dieses Risiko besonders groß, denn die Einfluss- und Kontrollmöglichkeiten entziehen sich den Verantwortlichen.

Auch für die Cloud gilt aber: Jedes Unternehmen unterliegt im Rahmen seiner Geschäftstätigkeit verschiedenen Gesetzen, branchenspezifischen Regelungen und eigenen Vorgaben zur ordnungsgemäßen Datenverarbeitung. Kommt ein Dienstleister ins Spiel, der Teile der IT-Infrastruktur, Anwendungen und Daten für das Unternehmen verwaltet und betreut, dehnt sich der Verantwortungsbereich auch auf diesen Dienstleister aus. Jedes Unternehmen muss sicherstellen, dass der Dienstleister vertrauenswürdig ist und die Compliance-Anforderungen eingehalten werden.

Verantwortung ist nicht delegierbar

Um es klar zu sagen: Wer Cloud-Services nutzt, delegiert damit nicht die Verantwortung für den Schutz der Daten an den Dienstleister. Beim Transport und der Verarbeitung von Mitarbeiter- oder Kundendaten müssen auch in der Cloud die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) eingehalten werden. Auf EU-Ebene gibt etwa die "Data Protection Directive" aus dem Jahr 1995 den Rahmen vor.

In Staaten außerhalb der EU herrscht häufig ein Datenschutz-Verständnis, das stark von der europäischen Linie abweicht. So sieht die EU-Richtlinie auch vor, dass vor einem Transfer personenbezogener Daten in Drittstaaten zu überprüfen ist, ob dort ein vergleichbares Niveau der Datenschutzbestimmungen vorliegt. Nur dann ist die Übermittlung zulässig.

Auch abgesehen von den gesetzlichen Anforderungen ist es im ureigenen Interesse eines Unternehmens, sicherzugehen, dass ein Dienstleister die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sicherstellt, die ihm anvertraut werden. Grundsätzlich sollten Verantwortliche deshalb vor der Entscheidung für einen Dienstleister die eigenen Anforderungen an Sicherheit und Compliance möglichst genau definieren.

Der Provider wiederum sollte in der Lage sein, seine Dienstleistungen auf die Compliance-Anforderungen des Kunden abzustimmen. Es muss dasselbe Datenschutzniveau bieten wie der Auftraggeber. Zudem muss sich der Nutzer von Cloud-Services regelmäßig selbst ein Bild von den technischen und organisatorischen Maßnahmen machen, mit denen der Service-Provider den Schutz von Daten seiner Kunden und die Einhaltung von Compliance-Vorgaben sicherstellt.

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.