security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Sicher in der Wolke – Studie zur Cloud-Computing-Sicherheit

Das Thema Cloud-Computing hat für Unternehmen in den vergangenen Jahren eine zunehmende Bedeutung erlangt und dazu geführt, dass Cloud-Services bereits in einer Vielzahl von Anwendungen für Endbenutzer eingesetzt werden. Die Motivation für Unternehmen, sich mit Cloud-Computing zu beschäftigen, begründet sich in den ständig wandelnden Herausforderungen, die mit einer wachsenden Dynamik des Marktes und einer zunehmenden Wettbewerbssituation einhergehen. Dies hat zur Folge, dass eine stetige Anpassung und Überprüfung des eingesetzten Wissens, der Technologie und insbesondere des eigenen Ressourceneinsatzes notwendig sind.

Dr. Werner Streitberger

Fraunhofer Institut für Sichere Informationstechnologie

In Unternehmen hat sich der Einsatz von rechenintensiver Informationstechnologie (IT) bereits für den Geschäftsbetrieb als unverzichtbar erwiesen, um Geschäftsprozesse besser auszurichten und neue Geschäftslösungen mit grösserer Flexibilität und höherer Geschwindigkeit bereitzustellen. Dieser Situation gegenüber stehen die Kosten für die Anschaffung, den Betrieb und die Wartung der IT. Diese Kosten rechtfertigen jedoch nur selten die vollständige Abdeckung des maximal erwarteten Bedarfs von Software und Ressourcen, wie Speicher und Rechenleistung. So müssen Unternehmen neben Effizienz- und Geschwindigkeitsverbesserungen auch Kosteneinsparungen und Verbesserungen der IT-Sicherheit für ihre Infrastruktur realisieren, um wettbewerbsfähig zu bleiben. Cloud-Computing kann hierzu den nächsten Schritt darstellen, IT-Dienste zu verbessern und bestehende Kapazitäten besser auszulasten. Das hinter Cloud-Computing stehende Konzept beschreibt verschiedene Lösungsansätze zur Umsetzung einer dynamischen Nutzung von IT-Ressourcen wie Speicherkapazität oder Rechenleistung und Diensten innerhalb eines Unternehmens und über Unternehmensgrenzen hinweg. Cloud-Computing-Systeme ermöglichen es, Infrastrukturressourcen und Anwendungsdienste bei Bedarf als IT-Service zu beziehen und damit Dienstleistungen in die Cloud auszulagern. Trotz der möglichen Produktivitäts- und Kostenvorteile zögern die meisten Unternehmen, z. B. sensible technische Berechnungen oder betriebliche Anwendungen per Cloud-Computing einem externen Dienstleister zu übertragen.

Die Hauptgründe sind Sicherheitsbedenken: Natürlich sollen beispielsweise die Ergebnisse einer Portfoliooptimierung einer Bank oder einer Crash-Test-Simulation während der Entwicklung eines neues Autos nicht dem Mitbewerber in die Hände fallen. Zusätzlich wächst

die Abhängigkeit von externen IT-Systemen, deren Ausfall durch technische Störungen, Schadsoftware oder Hackerangriffe nicht nur die Kommunikation, sondern auch ganze Geschäfts- oder Produktionsprozesse zum Stillstand bringen kann.
Da fast jeder grosse Anbieter von Cloud-Services in der Vergangenheit einen grösseren Vorfall im Bereich Verfügbarkeit oder Sicherheit hatte, ist das Fraunhofer SIT der Frage nachgegangen, wie sich IT-Sicherheit und der Trend zum Cloud-Computing vereinbaren lassen.
In einer der ersten Studien zu diesem Themenfeld hat das Fraunhofer SIT die Sicherheitsaspekte beim Cloud-Computing systematisch analysiert (vgl. http://www.sit.fraunhofer.de/cloud-security) und Risiko- und Themenfelder identifiziert, sowie eine erste Zusammenstellung von Do's and Dont's sowie Checklisten der 17 wichtigsten Sicherheitsaspekte von Cloud-Computing-Systemen erarbeitet.
Im Zusammenhang mit der Sicherheit von Cloud-Computing besteht noch eine Vielzahl offener Fragen. So ist beispielsweise noch nicht hinreichend untersucht, ob Erweiterungen bestehender Systeme ausreichen oder neue Sicherheitstechnologien für den Einsatz von Cloud-Computing-Systemen entwickelt werden müssen. Ein Beispiel hierfür ist die Datensicherheit.
Unter dem Begriff der Datensicherheit wird im Rahmen der Studie die Sicherheit aller Daten – inklusive eventuell vorhandener Konfigurations- und Metadaten – verstanden, die in Cloud-Computing-Systemen gespeichert, verarbeitet und zwischen Cloud-Computing-Systemen und deren Services transportiert werden. Dabei stehen die Schutzziele Vertraulichkeit und Integrität im Vordergrund.
Analog zum klassischen Auslagern der IT zu einem Outsourcing-Anbieter, der die Daten eines Unternehmens im Zuge des Auslagerns der IT übernimmt, werden die Daten eines Cloud-Benutzers ebenfalls auf den Rechnern eines Cloud-Anbieters gespeichert. Dies hat zur Folge, dass der Cloud-Serviceanbieter Sicherheitsfunktionen implementieren und bereitstellen muss, die diese Daten schützen, und gegebenenfalls dem Cloud-Benutzer Rechenschaft darüber ablegen muss.
Vor dem Übermitteln von Daten an einen Service eines Cloud-Anbieters sollte ein Cloud-Konsument eine Klassifikation seiner Daten vornehmen und genau festlegen, welche Daten bei einem Cloud-Anbieter gespeichert werden dürfen. In dieser Klassifikation muss genau spezifiziert werden, mit welchen Sicherheitsmassnahmen die Daten übermittelt und abgespeichert werden müssen. Dies können bestimmte kryptografische Verfahren oder aber auch Richtlinien sein, die ein Anbieter unterstützen muss. Zur Sicherstellung der Schutzziele bieten sich die Festlegung von Sicherheitsrichtlinien an, die vom Anbieter eingehalten werden müssen. In diesen Sicherheitsrichtlinien kann beispielsweise die Verwendung bestimmter Verschlüsselungstechnologien wie beispielsweise Public-Key-Infrastrukturen (PKI) vorgeschrieben werden.
Üblicherweise werden mit dem Cloud-Anbieter die Schlüssel für die sichere Übertragung und Speicherung der Daten ausgetauscht und diese auf den Daten angewandt. Zusätzlich kann durch einen Cloud-Konsumenten das Prinzip der Datenminimierung angewandt werden, bei dem z. B. Kundendaten aus den Datensätzen, die durch einen Cloud-Service verarbeitet werden, entfernt oder ersetzt werden und nur durch Daten, die unternehmensintern vorgehalten werden, wieder ihre ursprünglich semantisch Bedeutung erlangen. Ein solches Szenario kann beispielsweise bei rechenintensiven Statistikberechnungen angewandt werden, wo beispielsweise nur Zahlen für die Berechnung benötigt werden, die Zuweisung zu einem Kunden aber für die eigentliche Berechnung nicht notwendig ist.

Auszug aus der Checkliste der Datensicherheit

- Wo werden die Daten gespeichert und wie sind diese von den Daten anderer Kunden getrennt?
- Wo werden die Daten zusätzlich z. B. bei der Datensicherung und -archivierung oder durch Redundanz des Cloud-Computing-Systems gespeichert?
- Werden bei einer Löschung die Daten von allen Instanzen, allen Zwischenspeichern und allen Sicherungskopien gelöscht?
- Welche Verschlüsselungsverfahren bietet der Cloud-Anbieter an? Ist eine Verwendung dieser Verfahren im Vertrag festgeschrieben?
- Können Daten nach einer Löschung wiederhergestellt werden?
- Ist es möglich die Daten wieder in das Unternehmen zurückzuholen?