Iryna Tsvihun

Dr. Niels Fallenbeck

Cloud-Leitstand

Die Schaltzentrale für die Cloud

Trotz der wirtschaftlichen Attraktivität und des identifizierten Marktpotentials gilt die Nutzung von Cloud-Computing-Angeboten für Unternehmen besonders in Deutschland und Europa weiterhin als schwierig. Das liegt in erster Linie an den hohen Anforderungen hinsichtlich Datensicherheit, Compliance und Verfügbarkeit, denen Anbieter und Betreiber von Cloud-Infrastrukturen und -Diensten gegenüber stehen. Zusätzlich sind die Unternehmen auf Kundenseite durch die bekannt gewordenen Sicherheitsvorfälle der letzten Monate für die Sicherheitsthematik sensibilisiert worden. Folgende Fragen müsste sich daher jedes Unternehmen stellen:

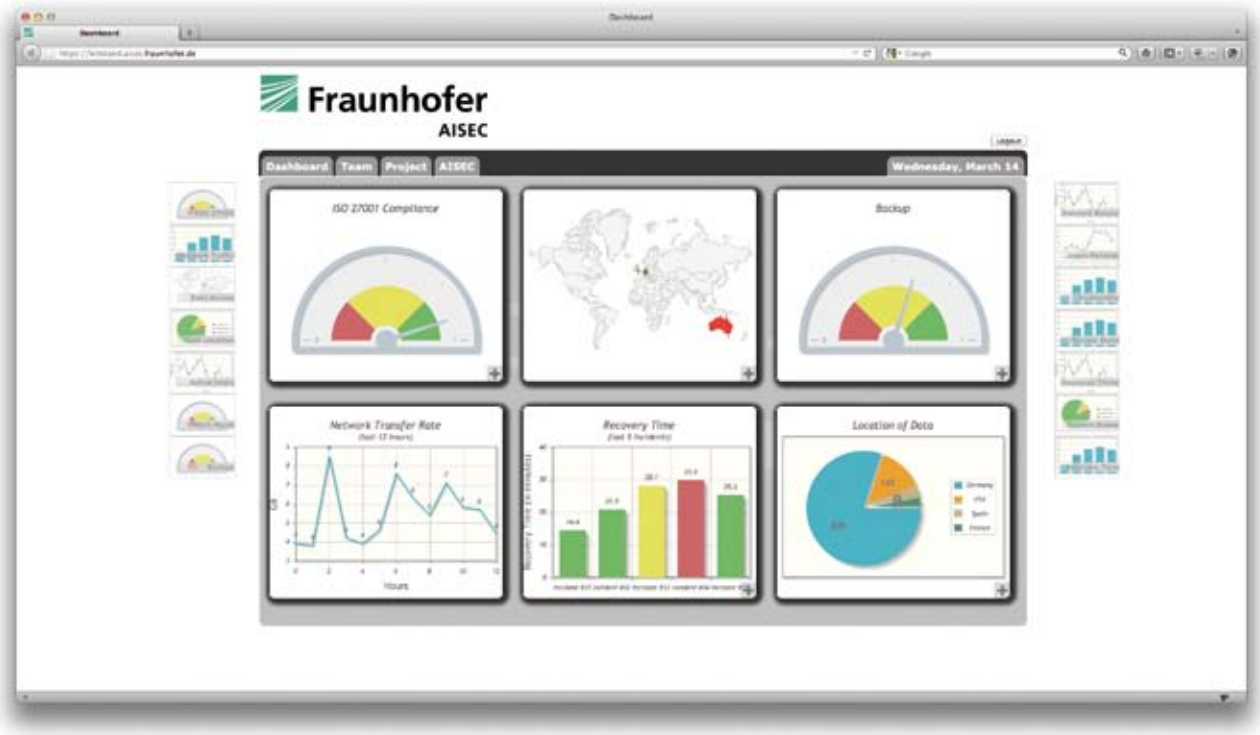
- Wo sind meine Daten und wer hat Zugriff auf diese?
- Wie sicher und verfügbar sind sie?
- Bin ich compliant gemäß den Anforderungen aus ISO 27001, BSI Grundschutz, SOX, PCI DSS, etc.?
- Wie kann die Sicherheit der Unternehmensdaten und -prozesse in der Cloud kontrolliert werden?

Diese Fragestellungen muss jeder IT-Verantwortliche bei der Einführung und Nutzung von Cloud-Computing beachten. Laut einer im Februar 2012 veröffentlichten Security-Umfrage von Retarus beklagen vier von fünf Sicherheitsverantwortlichen in mittelständischen und großen Unternehmen in Deutschland, Österreich und der Schweiz die mangelnde Transparenz bei Cloud-Angeboten. Nur etwa 20 Prozent der befragten Unternehmen wissen, wo ihre Daten physikalisch gespeichert und verarbeitet werden und welchen nationalen Gesetzen sie damit unterliegen.[1] Eine Welle der Verunsicherung ging durch die IT-Branche als bekannt wurde, dass der Patriot Act den US-amerikanischen Behörden den Zugriff auf Daten amerikanischer Unternehmen, ihrer internationalen Tochtergesellschaften sowie aller Unternehmen, die Server im Geltungsbereich der US-Gesetze betreiben, erlaubt, ohne dass die Eigentümer der Daten darüber informiert werden müssen. Dieser Kontrollverlust und die Tatsache, dass die Cloud-Nutzer auch nach der Auslagerung der Daten in die Cloud für die Einhaltung von Datenschutz und sonstigen Compliance-Anforderungen verantwortlich sind, stellt für viele Unternehmen eine bedeutende Hemmschwelle bezüglich der Nutzung von Cloud-Computing-Angeboten dar.

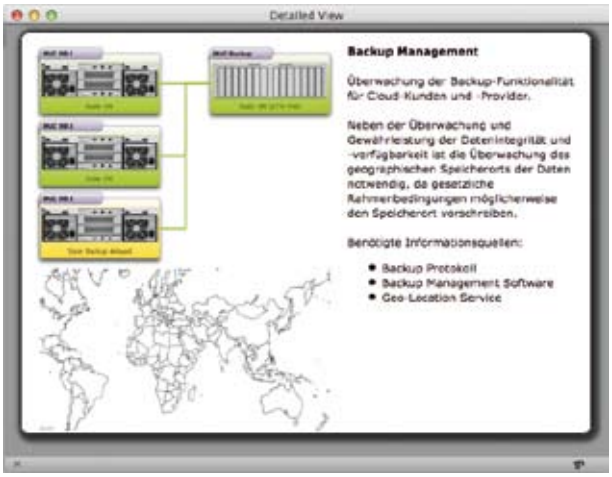
Auf der einen Seite müssen die drei Kernprinzipien der Sicherheit – Vertrauenswürdigkeit, Integrität und Verfügbarkeit – erfüllt und nachgewiesen werden. Auf der anderen Seite müssen alle länder- und branchenspezifischen gesetzlichen Richtlinien und Vorschriften, wie z. B. ISO- und BSI-Standards, Basel II und SOX (Sarbanes-Oxley Act) eingehalten werden. Darüber hinaus wird die Menge der zu verarbeitenden Daten täglich größer (Big Data) und sie werden von einer Vielzahl unterschiedlicher Endgeräten abgerufen und verarbeitet (Consumerization der IT).

Seitens der Cloud-Anbieter ist mehr Transparenz erforderlich, um Nutzern die notwendige Kontrolle und Übersicht über den spezifischen Status des in Anspruch genommenen Dienstes zu ermöglichen und so das Vertrauen in die Cloud-Angebote zu stärken. Nutzern fehlen vertrauensbildende Maßnahmen seitens der Cloud-Anbieter, mit denen die Anbieter in nicht abstreitbarer Art und Weise nachweisen und aufzeigen, dass alle Sicherheits- und Datenschutzanforderungen des Kunden durchgehend eingehalten werden. Insbesondere für international agierende Unternehmen und Konzerne ist es oft unerlässlich, Kundendaten nach verschiedenen länderspezifischen gesetzlichen Richtlinien und Vorschriften verarbeiten zu können oder sogar selbst zu bestimmen, wo und nach welchen Datenschutz- und Compliance-Regeln ihre Daten gespeichert und verarbeitet werden.

Damit Unternehmen jederzeit den Überblick über die eigenen Cloud-Anwendungen behalten, arbeitet Fraunhofer AISEC an einer Lösung zur Überwachung von Cloud-



Zentralansicht des Cloud-Leitstands: Übersicht über Cloud Security und Compliance



Backup Management auf einen Blick

Infrastrukturen, dem Cloud-Leitstand. Der Cloud-Leitstand ist eine Zentrale, in der alle risiko-, sicherheits- und Compliance-relevanten Informationen zusammenlaufen. Durch die Verknüpfung dieser unterschiedlichen Informationen wird die Verarbeitung und Speicherung von Daten und Prozessen in der Cloud beherrschbarer und transparenter. Die Überwachung schließt Prozesse, Applikationen und Infrastruktur in der Cloud ein und bietet einen Abgleich der technischen Informationen mit den Compliance-Vorgaben. Damit soll dem Kontrollverlust in der Cloud entgegengewirkt werden.

Der Cloud-Leitstand dient dem Cloud-Anbieter bzw. dem Cloud-Betreiber als Werkzeug, das mit Monitoring- und Managementsystemen für Governance, Risk und Compliance (GRC) wie z.B. RSA Archer kombiniert werden kann. Durch die Verknüpfung der aus den unterschiedlichen Quellen gewonnenen Informationen können Anforderungen, wie beispielsweise die Einhaltung der ISO 27001-Kontrollen, schnell und automatisiert beantwortet werden. Zusätzlich lassen sich neue Fragestellungen definieren und überwachen, wie z.B. die Einhaltung der Compliance-Vorgabe bzgl. des Orts der Daten. Darüber hinaus können die im Cloud-Leitstand verfügbaren Daten im Hinblick auf Anforderungen der Cloud-Anwender analysiert werden. So lassen sich individuelle Berichte bis hin zu automatisierten Benachrichtigungen (Alerts) bei Auftreten vorher festgelegter Ereignisse bereitstellen.

Die Darstellungsoberfläche des Cloud-Leitstands ist Mehrbenutzer-fähig: Jeder Benutzer des Cloud-Leitstands hat eigene Präferenzen, welche Informationen er in welcher Weise dargestellt haben möchte und eigene Anforderungen, welche Informationen in welcher Granularität er für die Ausführung seiner Aufgaben und zur Erstellung der Compliance-Nachweise für seine Kunden benötigt. Einen für die Cloud-Infrastruktur verantwortlichen Netzwerkadministrator interessiert eine detaillierte Darstellung der auf Netzwerkebene gewonnenen Daten, während ein Prozessbesitzer am Gesamtzustand des Prozesses und an den Zugriffen auf die im Prozess verarbeiteten Daten interessiert ist. Ein Auditor kann mit Hilfe des Cloud-Leitstands auf die für Prüfung notwendigen Informationen zugreifen und damit den Audit- bzw. Zertifizierungsprozess beschleunigen.

Der Cloud-Leitstand zielt auf die Herstellung einer umfassenden Transparenz in der Cloud-Umgebung in Bezug auf IT-Sicherheit und Einhaltung von Compliance-Vorgaben der Cloud-Nutzer ebenso wie der Cloud-Anbieter. Des Weiteren trägt er zur Erhöhung der Kontrollierbarkeit der Cloud durch den Betreiber bei, sodass er die gewünschten vertrauensbildenden Maßnahmen seinen Kunden anbieten und selbst die Einhaltung der gegebenen Garantien z.B. im Rahmen von Service Level Agreements (SLAs) überwachen kann. Der Cloud-Leitstand ermöglicht dem Cloud-Anbieter durch eine effiziente Überwachung seiner Systeme, z.B. hinsichtlich sicherheitskritischer Ereignisse, und eine intelligente Verknüpfung aller verfügbaren Informationen Aussagen zu den individuellen Fragestellungen der Cloud-Nutzer zu liefern. Durch die damit verbundene Erhöhung der Transparenz von Cloud-Computing-Angeboten soll die Akzeptanz solcher Angebote auf Anwenderseite gesteigert und die Sorge vor Kontrollverlust genommen werden.

Dipl-Kffr., M.Sc. Iryna Tsvihun
E-Mail: Iryna.Tsvihun@aisec.fraunhofer.de

Dr. Niels Fallenbeck
E-Mail: Niels.Fallenbeck@aisec.fraunhofer.de

Internet: www.aisec.fraunhofer.de
www.cloud-competence-center.de

[1] http://www.retarus.com/de/presscenter/messages/2012_02_01_fachinformation_cloud.php