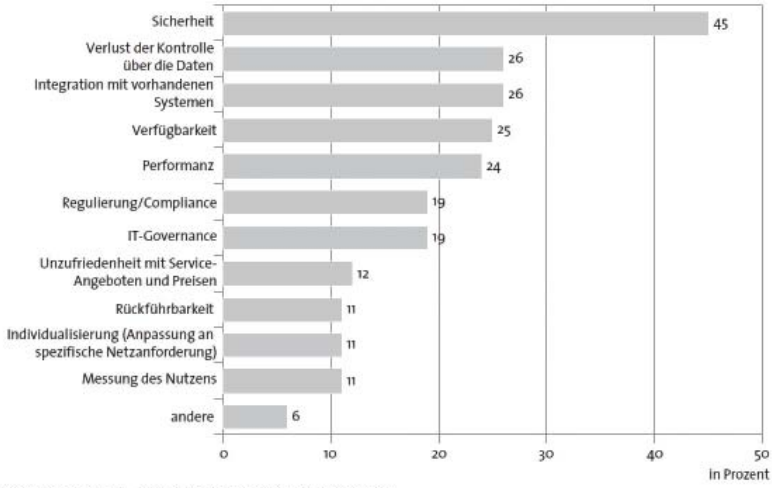
Cloud Security – Sicherheit in der Wolke

Iryna Tsvihun **Gerd Stefan Brost**

Bei Cloud-Computing-Systemen mieten Unternehmen Infrastrukturressourcen und Anwendungsdienste von Dienstleistern an und bezahlen nur die tatsächlich verbrauchten Ressourcen. Möglich machen das Virtualisierungstechnologien und serviceorientierte, verteilte Softwaresysteme. Mit ihrer Hilfe lassen sich Cloud-Ressourcen dynamisch als IT-Service beziehen und Dienstleistungen in die Cloud auslagern. Unternehmen können auf eigene IT-Infrastrukturen verzichten und bleiben dennoch hochflexibel. Durch das Auslagern von Ressourcen und Diensten kommt es jedoch zu Informationsasymmetrien, die im schlimmsten Fall zu einem Kontrollverlust der Daten in Cloud-Systemen resultieren. Eine weitere Gefahr ist die Nichtverfügbarkeit der angemieteten Ressourcen und Services, die starke Auswirkungen auf die Geschäftsprozesse von Unternehmen haben können. Weitere zentrale Herausforderungen im Cloud Computing sind die Erfüllung der klassischen Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität) sowohl auf der Anwender- als auch auf der Anbieterseite, IT-Governance, Compliance und Datenschutzbestimmungen, sowie fehlende Standardisierung und Performanz der Cloud-Services. Dies bestätigt auch die Untersuchung der Erfolgsfaktoren von Cloud Computing aus CIO-Sicht (vgl. Abbildung 1).



Quelle: BITKOM: Leitfaden Cloud Computing - Was Entscheider wissen müssen (Dezember 2010)

Abbildung 1: Erfolgsfaktoren von Cloud Computing aus CIO-Sicht

Diesen und weiteren Cloud-Sicherheits-Herausforderungen, die in einer zögernden Nutzung der Cloud-Systeme durch Unternehmen resultieren, stellt sich das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) mit dem Forschungsbereich „Sichere Services & Qualitätstests" in Garching bei München. Das Fraunhofer-Institut SIT ist ein unabhängiger Spezialist für IT-Sicherheit und Sicherheit durch IT. 150 hochqualifizierte Mitarbeiter, die u.a. in den Forschungsbereichen Sicherheit der eingebetteten Systeme, Hardware- und Netzwerksicherheit arbeiten, entwickeln unmittelbar einsetzbare Lösungen, die vollständig auf die Bedürfnisse der Auftraggeber ausgerichtet sind. Das Fraunhofer-Institut SIT ist für Unternehmen aller Branchen, sowie öffentliche Hand tätig. Viele erfolgreiche Projekte mit internationalen Partnern sind eindrucksvoller Beweis für eine vertrauensvolle und zuverlässige Zusammenarbeit.

Der Forschungsbereich „Sichere Services & Qualitätstests" des Fraunhofer-Instituts SIT verfügt in Garching bei München über ein eigenes Cloud-Security-Testlabor, in dem Funktions-, Portabilitäts- und Interoperabilitätstests sowie die Entwicklung von Sicherheitskomponenten und Referenzimplementierungen durchgeführt werden. Hierbei werden alle Entwicklungsphasen eines Cloud-Ökosystems vom Entwurf einzelner Dienste über Prototypen bis hin zum (Sicherheits-)Test marktreifer Gesamtsysteme betrachtet. Darüber hinaus unterstützt das Fraunhofer-Institut SIT Kunden bei der Analyse möglicher Schwachstellen und Bedrohungen, sowie entwickelt diverse Verfahren für Cloud Management und Monitoring (vgl. Abbildung 2). Der Forschungsbereich hat bereits mehrere Studien zur Sicherheit von Cloud Computing verfasst und ist an zahlreichen nationalen und internationalen Forschungs- und Entwicklungsaktivitäten beteiligt. Projektpartner profitieren hierbei von langjähriger Erfahrung in SOA-Security, dem sicheren Cloud Computing sowie dem verteilten Management digitaler Identitäten. Das Fraunhofer-Institut SIT ist aktives Mitglied in der Cloud Security Alliance, dem BITKOM, dem EuroCloud-Verband, dem TeleTrusT und der Kantara Initiative.

Zu den neusten Entwicklungen des Cloud-Security-Testlabors zählen das Cloud Cockpit, das erstmals auf der CeBIT 2011 vorgestellt wurde, sowie das aktuelle Projekt Sealed Cloud.

Cloud Cockpit

Die Nutzung des Cloud Computing verzögert sich durch die Ungewissheit in Sachen Datensicherheit, Compliance und Verfügbarkeit. Damit Unternehmen technische und organisatorische Sicherheitsanforderungen auch in der Cloud erfüllen können, hat das Fraunhofer-Institut SIT in Garching bei München Lösungen zur Datenverschlüsselung, Datenüberwachung und automatischen Datenverschiebung in der Cloud entwickelt.

Beim Cloud Computing wandern die Informationen oft automatisch von Server zu Server. Damit Unternehmen das Risiko für ihre Daten dennoch einschätzen und kontrollieren können, werden Lösungen entwickelt, mit denen sich das Sicherheitsniveau von Cloud-Angeboten messen und Daten in der Cloud schützen lassen. Grundlage bildet ein innovatives Verschlüsselungskonzept, das Informationen vor dem unbefugten Zugriff Dritter schützt und nur bei Bedarf diejenigen Informationen entschlüsselt, die wirklich benötigt werden. Zur Messung der Sicherheit von Cloud-Diensten entwickelt das Fraunhofer-Institut SIT spezielle Sicherheitsmetriken. Diese beinhalten Messwerte zur Verfügbarkeit und anderen überprüfbaren Sicherheitsmaßnahmen, mit denen das Security Level des Anbieters festgestellt werden kann. Dadurch können Unternehmen prüfen, ob das jeweilige System den eigenen Anforderungen genügt. Falls nicht, lassen sich die Daten von einer Cloud in eine andere verschieben.

Abbildung 2: Cloud Security Angebot

Um Arbeitsweise und Entwicklungsstand der unterschiedlichen Lösungen zu demonstrieren, wurden die verschiedenen Werkzeuge unter einer Oberfläche zusammengefasst. In diesem Cloud Cockpit laufen alle Informationen zusammen und die Wirkung der angebrachten Schutzmaßnahmen lässt sich beobachten. Das Cockpit zeigt das Sicherheitsniveau von Cloud-Systemen und erlaubt, die Daten zwischen verschiedenen Angeboten zu verschieben. Das Cloud Cockpit präsentiert beispielhaft die Betreibermodelle Private Cloud, Community Cloud und Public Cloud, die sich in ihren Sicherheitseigenschaften unterscheiden.

Sealed Cloud

Das Fraunhofer-Institut SIT in Garching bei München gehört zusammen mit der SecureNet GmbH und der Uniscon GmbH zu den Gewinnern des Technologiewettbewerbs „Trusted Cloud" des Bundesministeriums für Wirtschaft und Technologie (BMWi). Die Kooperationspartner entwickeln im Rahmen des Projekts die so genannte „Sealed Cloud"-Plattform für Privatpersonen, Unternehmen und den öffentlichen Sektor. Ziel des Vorhabens ist die Realisierung einer technisch „versiegelten" Cloud-Infrastruktur, in der der Betreiber nicht auf die Daten seiner Kunden zugreifen kann. Dadurch bietet Sealed Cloud durchgängigen Schutz der Daten. Die besondere Innovation liegt hier im Ausschluss der bekannten Schwachstelle Mensch, d.h. des Personals des Betreibers der Cloud.

Viele Fragen im Bereich Cloud Sicherheit sind bis heute unbeantwortet wie z.B.: Wer hat Zugriff auf den Server? Gibt es nur eigene Administratoren oder auch externe Dienstleister? Wie sind die internen Prozesse gestaltet und wie abgesichert? Sind die Daten verschlüsselt? Wer hatte oder hat Zugang zu den Dekodierungsschlüsseln? Die Ungewissheit im Rahmen dieser Fragestellungen hält die Unternehmen bis heute davon ab, Cloud-Systeme zu nutzen. Die Sealed Cloud kombiniert die ökonomischen Vorteile einer über das Internet nutzbaren Public Cloud mit der Sicherheit einer abgeschotteten Private Cloud. Diese verhindert mittels technischer Verfahren und Vorrichtungen, dass der Betreiber der Cloud, sein Personal oder externe Dritte auf Daten seiner Kunden zugreifen können. Dieser Schutz wirkt in allen Phasen der Verarbeitung. Damit schafft die Sealed Cloud „das noch fehlende Vertrauen durch Technik" und leistet einen entscheidenden Beitrag zur Datensicherheit der Cloud-Systeme.

Dipl-Kffr., M.Sc. Iryna Tsvihun
Iryna.Tsvihun@sit.fraunhofer.de

M.Sc. Gerd Stefan Brost
Gerd-Stefan.Brost@sit.fraunhofer.de

http://www.sit.fraunhofer.de
http://www.cloudsecuritylab.de