1 Executive Summary

Die vorliegende Studie zum Thema Cloud-Computing-Sicherheit zielt darauf ab, einen umfassenden Rahmen zur Betrachtung der Sicherheitsproblematik in Cloud-Computing-Systemen zu geben. Adressaten der Studie sind Entscheider in Unternehmen aller Branchen, die aktuell IT-Dienste ausgelagert haben, Cloud-Services bereits einsetzen oder in naher Zukunft einen Einsatz von Cloud-Services in Erwägung ziehen. Weitere Adressaten der Studie sind alle an der Thematik interessierten Personen sowie Anwender, die einen Überblick über Sicherheitsrisiken beim Einsatz von Cloud-Computing-Systemen und über aktuelle Cloud-Computing-Angebote sowie deren Kosten und Sicherheitslösungen gewinnen möchten.

Im Folgenden werden die Ergebnisse kurz vorgestellt und Hinweise gegeben, die aus Sicherheitssicht beim Einsatz von Cloud-Services beachtet werden sollten:

- Das Thema Sicherheit und Verfügbarkeit von Cloud-Computing-Systemen sind eine der wichtigsten Themen, die in jedem Cloud-Projekt betrachtet werden müssen. Fast jeder große Anbieter von Cloud-Services hatte in der Vergangenheit einen größeren Vorfall in einem der beiden genannten Gebiete.
- Kleine und mittlere Unternehmen (KMU) können ihre Sicherheit durch den Einsatz von Cloud-Services erhöhen, da sie zum einen die Möglichkeit haben, Sicherheitslösungen als Service von spezialisierten Anbietern beziehen zu können, und zum anderen von der Erfahrung des Anbieters in der Implementierung und im Betrieb von sicheren Services zu profitieren. Voraussetzung hierfür ist jedoch die Auswahl eines zertifizierten und vertrauenswürdigen Anbieters, dessen Cloud-Services auf Grundlage eines jederzeit überprüfbaren Service-Level-Agreements erbracht wird.
- Große Unternehmen sollten individuell die Sicherheitsfunktionen eines Cloud-Anbieters prüfen und im Einzelfall entscheiden, ob die verfügbaren Sicherheitsmechanismen für den konkreten Anwendungsfall ausreichend sind.
- Vorteile für den Einsatz von Cloud-Computing-Systemen basieren vor allem auf der Ausnutzung von Skaleneffekten zur Kosteneinsparung, der Möglichkeit, Kapazitäten dem aktuellen Bedarf anzupassen, und neuen Einsatzmöglichkeiten in der Organisation bestehender Prozesse.

- Risiken bestehen im Bereich der Sicherheit und Verfügbarkeit der Cloud-Services sowie möglichen Lock-In-Effekten, die bei der Auswahl eines Service auftreten können und hohe Kosten nach sich ziehen, wenn beispielsweise der Service eines Cloud-Anbieters gewechselt wird und durch geringe Standardisierung große Änderungen am bestehenden System vorgenommen werden müssen. Im Bereich Sicherheit und Verfügbarkeit sind die Schutzziele der IT-Sicherheit Vertraulichkeit, Integrität, Authentizität, Zurechenbarkeit, Verbindlichkeit, Verfügbarkeit und Schutz der Privatsphäre anzuwenden und während der Ableitung der Anforderungen festzulegen.
- Die Schutzziele der IT-Sicherheit lassen sich auch auf Cloud-Computing-Systeme übertragen. Sie sind jedoch für die genaue Betrachtung der Cloud-Computing-Systeme und ihre unterschiedlichen Ausprägungen zu allgemein, so dass sie für jeden Cloud-Service neu überprüft und angewandt werden müssen. Der Grund hierfür liegt in einer wenig standardisierten Vorgehensweise bei der Auswahl und dem Einsatz von Sicherheitstechnologien in Cloud-Computing-Systemen.
- Der Aufbau von Cloud-Computing-Systemen in seine vier Schichten Benutzer-, Software-, Plattform- und Infrastrukturschicht und die auf den Schichten agierenden Akteure bilden einen sehr komplexen Rahmen für die IT-Sicherheit. In dieser Studie werden alle wichtigen Schichten und Akteure vorgestellt, die je nach Anwendungsfeld und ausgewähltem Cloud-Service untersucht werden müssen.
- Für Cloud-Computing-Systeme werden zertifizierte Vorgehensmodelle und standardisierte Schnittstellen und Protokolle benötigt, die Cloud-Services zu Grunde liegen. Dies erhöht die Portabilität und Interoperabilität einzelner Cloud-Serviceangebote. Hierfür werden Standardisierungsgremien, Referenzimplementierungen und auf Cloud-Computing-Systeme angepasst Entwicklungsumgebungen benötigt.
- Die Cloud-Sicherheitstaxonomie gibt einen übersichtlichen Rahmen der Sicherheitsfelder, die beim Einsatz von Cloud-Services betrachtet werden sollten. Wegen der schnellen Weiterentwicklung der Technologien und der bestehenden Serviceangebote sollte die Anwendung der Cloud-Taxonomie projektbezogen erfolgen und die Gewichtung einzelner Sicherheitsfelder nach der jeweiligen Anforderung angepasst werden.
- Die aktuellen Cloud-Serviceangebote zeigen, dass vor allem im Bereich der Infrastruktur eine Reihe von Sicherheitstechnologien bereits zum Einsatz kommen. In den Bereichen Architektur, Verwaltung und Compliance ist die Unterstützung von Sicherheitstechnologien seitens der Cloud-Anbieter jedoch noch nicht soweit fortgeschritten, um die geforderten Schutzziele zu erreichen. Hier sind weitere, detaillierte Analysen notwendig, um heraus zu finden, welche aktuellen Technologien hier eingesetzt werden können und ob neue Technologien hierfür entwickelt werden

müssen. Es zeigt sich ein Trend, bestimmte Sicherheitsfunktionen wie beispielsweise Teile der Identitäts- und Zugangsverwaltung von spezialisierten Anbietern als Service zu beziehen.

- Im Bereich der Verwaltung sind Service-Level-Agreements ein wichtiger Bestandteile zur Festschreibung aller Rechte und Pflichten zwischen den Cloud-Benutzern und Cloud-Anbietern. Die bisher angebotenen standardisierten Service-Level-Agreements, die ein Cloud-Benutzer meist nicht frei verhandeln und nur akzeptieren oder ablehnen kann, geben nur minimale Garantien bezüglich der Dienstgüte eines Cloud-Services. Vor allem Sicherheitsgarantien sind nur rudimentär in diesen Service-Level-Agreements vorhanden und müssen ausgebaut werden, um die eingangs vorgestellten Schutzziele zu erreichen. Zusätzlich werden Systeme benötigt, die eine automatisierte Überwachung und Prüfung der vereinbarten Dienstgütekriterien zulassen.
- Aus Sicht der Compliance können Cloud-Services eingesetzt werden. Jedoch bleibt die Verantwortung der Daten meist beim Cloud-Benutzer, so dass dieser genaue Richtlinien definiert sollte, welche Daten wie in einem Cloud-Service abgespeichert und verarbeitet werden dürfen und welche Sicherheitsfunktionen vorhanden sein müssen. Auch aus rechtlicher Sicht sollte im Einzelfall überprüft werden, welche Einschränkungen bei bestimmten Daten gelten und die Verwendung eines Cloud-Services in Betracht gezogen werden kann.
- Die Marktübersicht der Studie gibt einen Überblick über ausgewählte Cloud-Serviceangebote, ihre Preise und Funktionen. Des Weiteren wird die Taxonomie des sicheren Cloud-Computing auf diese Cloud-Services angewandt und deren Sicherheitsfunktionen untersucht. Dabei lässt sich festhalten, dass die Informationen zu den implementierten Sicherheitsfunktionen durch die Cloud-Anbieter nur unzureichend dokumentiert sind. Häufig nimmt die Sicherheit bei der Vorstellung ihrer Angebote nur eine untergeordnete Rolle ein, so dass hier vor der Auswahl und Nutzung eines Cloud-Services beim Anbieter detaillierte Informationen angefordert werden sollten und eventuell ein Proof-of-Concept vor dem eigentlichen Produktiveinsatz eines Cloud-Services realisiert werden sollte.