Cloud Computing Security – Nachweis der Sicherheit beim Anbieter durch Zertifizierung

Dr. Clemens Doubrava **Isabel Münch**

Cloud Computing verspricht eine hohe Flexibilität und Effizienz sowie sinkende Kosten bei der Bereitstellung und Nutzung von IT. Allerdings erfordern sensible Daten, Anwendungen und Prozesse ein hohes Maß an Informationssicherheit.

Auslagerung von IT in die Cloud bedeutet, dass sich Cloud-Kunden in eine starke Abhängigkeit von den jeweiligen Cloud-Dienstleistern begeben – schließlich haben sie dadurch keinen direkten Zugriff mehr auf Hard- und Software. Bevor Unternehmen oder Behörden Daten in die Cloud verlagern, sollten sie sich vorher davon überzeugen, dass der ausgewählte Dienstleister alle Anforderungen des Kunden im Hinblick auf Informationssicherheit und Datenschutz erfüllt. Dafür müssen die Kunden natürlich ihre Sicherheits- und Datenschutz-Anforderungen auch konkret benennen können. Bevor Unternehmen und Behörden die Auslagerung von Informationen bzw. Aufgaben in Angriff nehmen, sollten sie klare Sicherheitsziele und -leitlinien festgelegt haben. Dafür müssen sie auch wissen, welche Informationen in ihrer Institution schützenswert sind. Vor einer Auslagerung sollten also Informationen und Geschäftsprozesse in Bezug auf ihren Schutzbedarf, also in Punkto Vertraulichkeit, Integrität und Verfügbarkeit, klassifiziert werden. Diese Klassifikation ist wesentliche Voraussetzung für die spätere Auswahl und Anwendung adäquater Sicherheitsmaßnahmen in den verschiedensten Bereichen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit)“ veröffentlicht, um sinnvolle und

Sicherheitsmanagement beim Anbieter	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Definiertes Vorgehensmodell für alle IT-Prozesse (z. B. nach ITIL, COBIT)	✓			✓		
Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. nach BSI-Standard 100-2 (IT-Grundschutz), ISO 27001)	✓			✓		
Nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud	✓			✓		
Nachweis einer ausreichenden Informationssicherheit (Zertifizierung)		✓	✓		✓	✓
Angemessene Organisationsstruktur für Informationssicherheit beim CSP (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)	✓			✓		

umsetzbare Sicherheitsanforderungen an Cloud-Computing-Angebote aufzuzeigen. Mit dem Eckpunktepapier bietet das BSI außerdem eine solide fachliche Basis, auf der Sicherheitsfragen zwischen Cloud-Computing-Anbietern und Cloud-Anwendern diskutiert werden können. Unternehmen und Behörden können dieses Papier auch nutzen, um darauf aufbauend konkrete Empfehlungen zur Absicherung von Cloud-Services zu erarbeiten.

Das Eckpunktepapier deckt elf als kritisch identifizierte Bereiche der Cloud-Computing-Sicherheit ab und enthält darüber hinaus eine Reihe von Best Practices für die Absicherung dieser Bereiche. Neben Sicherheitsanforderungen aus der klassischen IT wie Sicherheitsarchitektur, ID- und Rechtemanagement, Notfallmanagement, Monitoring und Security Incident Management werden auch Themen behandelt, die bei der Auslagerung von Daten, Anwendungen und Prozessen in eine Public Cloud besondere Relevanz erhalten. Hierzu zählen beispielsweise Themen wie Vertragsgestaltung, Datenschutz und Mandantenfähigkeit. Insbesondere ist die sichere und verlässliche Trennung der Mandanten aufgrund der gemeinsam genutzten IT-Infrastruktur essentiell und stellt einen Schlüsselaspekt der Cloud-Computing-Sicherheit dar.

Die Sicherheitsempfehlungen des Eckpunktepapiers orientieren sich außerdem am Schutzbedarf der in der Cloud verarbeiteten Informationen. Einen hohen Schutzbedarf in Bezug auf Vertraulichkeit haben beispielsweise vertrauliche Unternehmensinformationen oder schützenswerte personenbezogene Daten, hohe Verfügbarkeit wird beispielsweise bei geschäftskritischen Prozessen gefordert. Die Festlegung des Schutzbedarfs von Informationen, Anwendungen und IT-Systemen basiert dabei auf den Schutzbedarfskategorien nach IT-Grundschutz.

Unabhängig von nachgewiesener Sicherheit beim Cloud-Computing-Anbieter sollten die Kunden darauf achten, dass sie ihre Daten jederzeit aus der Cloud zurück bekommen können, damit kein „vendor lock-in“ entsteht. Um Interoperabilität zu gewährleisten, sollten die Anbieter von Cloud-Diensten standardisierte oder offen gelegte Schnittstellen (API, Protokolle) verwenden.

Sicherheitsmanagement als Basis für die Cloud-Sicherheit

Basis für ein zuverlässiges und sicheres Cloud Computing ist ein professionelles Management der Informationssicherheit (Information Security Management System, ISMS) auf Seiten des Cloud-Anbieters. Das BSI empfiehlt, sich am ISO-Standard 27001 oder bevorzugt am IT-Grundschutz auf der Basis von ISO 27001 zu orientieren. So ist schon ein großer Teil der Sicherheitsforderungen adressiert und abgedeckt. Als Nachweis für die Umsetzung eines ISMS dienen Zertifikate auf Basis der genannten Standards.

Nichtsdestotrotz gibt es beim Cloud Computing weitere Herausforderungen, wie zum Beispiel die Verfügbarkeit der angebotenen Dienste, die durch die oben genannten Zertifikate nicht notwendigerweise abgedeckt sind.

Sicherheitsarchitektur

Rechenzentren sind die technische Basis von Cloud Computing. Insofern ist es wichtig, dass jeder Anbieter die Sicherheit seiner Anlagen nach dem aktuellen Stand der Technik gewährleistet. Dazu zählen eine permanente Überwachung der Zugänge (etwa mit Videoüberwachungssystemen), Bewegungssensoren, Alarmsystemen und Sicherheitspersonal. Alle Versorgungskomponenten, die für den Betrieb unverzichtbar sind, sollten redundant ausgelegt sein (zum Beispiel Stromversorgung, Klimatisierung und Internetanbindung). Auch

zeitgemäße Vorkehrungen für den Brandschutz (Sensoren, Löschanlagen) zählen zu den Mindestanforderungen. Um die Sicherheit von Rechenzentren nachzuweisen, können neben ISO 27001-Zertifikaten auch spezielle Zertifikate wie TIA-942 bzw. Gütesiegel (z. B. eco Datacenter Star Audit) hilfreich sein.

Datenschutz und Compliance, Sicherheitsprüfungen beim Cloud-Anbieter
Unternehmen und Behörden unterliegen einer Reihe von Gesetzen, Verordnungen und Vorschriften, die vorschreiben, wie die verarbeiteten Daten abzusichern sind. Dazu gehören unter anderem Datenschutzregelungen, wie das Bundesdatenschutzgesetz (BDSG) oder die EU-Datenschutzrichtlinie 95/46/EG. Cloud-Computing-Anbieter können die Einhaltung von Datenschutzanforderungen beispielsweise über das Datenschutz-Gütesiegel des ULD nachweisen oder auf europäischer Ebene mit EuroPriSe, dem European Privacy Seal for IT Products and IT-Based Services.

Durch die Auslagerung von Daten oder Anwendungen in die Cloud begeben sich die Kunden in eine Abhängigkeit von der IT des Cloud-Anbieters. Daher müssen sie sich auf dessen Sicherheitsmaßnahmen verlassen können. Nachweise für das hohe Niveau der infrastrukturellen, technischen und organisatorischen Vorkehrungen beim Cloud-Computing-Anbieter sollten darum regelmäßig erbracht werden.

Cloud Zertifizierung
Derzeit existiert noch keine international anerkannte Zertifizierung für Cloud-Anbieter, auch wenn es an Initiativen nicht fehlt. So beschäftigen sich beispielsweise bei ISO zwei Gremien, SC27 und SC38, damit, Standards zur Sicherheit und Interoperabilität von Cloud Computing zu entwickeln. Auch das BSI wirkt hieran aktiv mit. Um das Sicherheitsniveau bei einem Cloud-Computing-Anbieter einschätzen zu können, müssen Kunden daher derzeit noch andere Wege nutzen. Sie könnten zur Beurteilung des Sicherheitsniveaus beispielsweise das Eckpunktepapier des BSI heranziehen und den Anbieter zur Einhaltung der dort beschriebenen Sicherheitsempfehlungen verpflichten. Der Cloud-Anbieter könnte den Kunden auch durch unabhängige Dritte erstellte Auditberichte vorlegen. Spezielle Aspekte der Informationssicherheit können bei höherem Schutzbedarf auch durch gesonderte Zertifizierungen nachgewiesen werden. Um beispielsweise das Sicherheitsmanagement bei Cloud-Computing-Providern beurteilen zu können, empfiehlt das BSI, sich die angemessene Umsetzung durch eine ISO 27001 Zertifizierung (zum Beispiel auf Basis des IT-Grundschutzes) nachweisen zu lassen. Die Sicherheit kritischer IT-Komponenten wie eines Hypervisors kann beispielsweise durch Zertifizierungen auf Grundlage der „Common Criteria for Information Technology Security Evaluation (ISO 15408)“ überprüft werden. Um alle zu prüfenden Aspekte beim Cloud Computing abzudecken, hat außerdem EuroCloud Deutschland ein SaaS-Gütesiegel entwickelt. Dies umfasst die Bereiche Vertrag und Compliance, Sicherheit, Betrieb und Infrastruktur, Prozesse, Anwendung und Implementierung.

Bei besonders hohen Anforderungen an Vertraulichkeit und Verfügbarkeit der Dienste empfiehlt das BSI, sich auch von den Subunternehmern des Cloud-Computing-Anbieters Sicherheitsnachweise vorlegen zu lassen.

Klare Rahmenbedingungen für Cloud Computing
Cloud Computing ermöglicht eine enorme Flexibilität bei der Nutzung von IT-Kapazitäten, wodurch sich viele Unternehmen und Behörden Kosteneinsparungen versprechen. Ein weiterer Vorteil ist die allgegenwärtige Verfügbarkeit von Geschäftsanwendungen.

Vertrauen in die Provider und ihre Angebote wird derzeit als wesentliche Motivation genannt, wenn nach den Gründen gefragt wird, warum sich potentielle Kunden für oder gegen Cloud-Angebote entscheiden. Vertrauen basiert auf der Einschätzung, ob ein Anbieter alle Risiken ausreichend, angemessen und nachhaltig abgedeckt hat, sowohl diejenigen aus dem Bereich der Informationssicherheit als auch aus Bereichen wie Datenschutz, Technik und Recht. Das erreichte Sicherheitsniveau sollte durch Prüfungen oder Zertifizierungen auf Grundlage etablierter Standards durchgeführt werden.

Generell ist festzustellen, dass Cloud-Computing-Anbieter, die stimmige Sicherheitsmaßnahmen auf unterschiedlichen Ebenen umgesetzt haben, diese den Kunden gerne vorstellen und sie auch auditieren oder zertifizieren lassen. Bleibt ein Cloud-Computing-Anbieter hier Antworten schuldig, sollte im Sinne einer konservativen Risikoabschätzung davon ausgegangen werden, dass der Anbieter die nachgefragten Sicherheitsmaßnahmen nicht umgesetzt hat.

Dr. Clemens Doubrava
E-Mail: clemens.doubrava@bsi.bund.de

Isabel Münch
E-Mail: isabel.muench@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)