Sicherheit und Cloud Computing

Iryna Windhorst

Dr. Niels Fallenbeck

Einführung

Der Großteil der Anwender, die sich im Internet bewegen, verwenden bewusst oder unbewusst bereits Cloud-Dienste, z.B. um ihr iPhone und ihren Computer über Apples iCloud zu synchronisieren. Es gibt bereits eine kaum überschaubare Anzahl von Cloud-Angeboten beginnend bei virtuellen Servern bis hin zu Textverarbeitungsprogrammen oder CRM-Suiten, die Anwender heute per Mausklick aus dem Internet beziehen können. Dabei muss zwischen der Private Cloud, die nur einem bestimmten Nutzerkreis wie Angehörigen der gleichen Firma offensteht, und der Public Cloud unterschieden werden, die von allen Interessierten verwendet werden kann. Durch die einfache Benutzbarkeit bestehender Cloud-Dienste erhalten diese auch (oft von den IT-Sicherheitsverantwortlichen unbemerkt) Einzug ins Unternehmen, indem Anwender Daten mit ihren Kollegen über einen Cloud-Speicherdienst wie z.B. Dropbox teilen oder die Dokumente im Google Docs gemeinsam bearbeiten. Ein Sicherheitsverantwortlicher sollte die Mitarbeiter seines Unternehmens bezüglich der Gefahren und Herausforderungen bei der Nutzung von Cloud-Services sensibilisieren. Das könnte beispielsweise über eine Awareness Kampagne geschehen.

Grundsätzlich kann man zwischen drei unterschiedlichen Service-Modellen unterscheiden: Infrastructure-as-a-Service (IaaS) stellt dem Anwender Infrastruktur wie virtuelle Maschinen oder Speicherplatz zur Verfügung, während Platform-as-a-Service (PaaS) eine Ausführungs- und Entwicklungsumgebung bereitstellt. Bei Software-as-a-Service (SaaS) schließlich stellt der Cloud-Anbieter ein gesamtes Softwareprodukt wie beispielsweise eine Textverarbeitung oder Projektmanagementunterstützung zur Verfügung, die der Anwender z.B. über seinen Webbrowser nutzen kann.

Bedrohungen

Um Cloud-Services nutzen zu können, müssen diese über das Internet erreichbar sein. Durch den Betrieb der Angebote durch Dritte und wegen der in der Cloud gespeicherten, teilweise sensitiven Daten und der guten Netzanbindung der Cloud-Services bieten diese ein attraktives Ziel für Angriffe. Die Cloud Security Alliance (CSA)[1] hat die aus ihrer Sicht sieben wichtigsten Gefahren bei der Nutzung von (Public) Cloud Computing beschrieben:

Missbrauch und schädliche Nutzung von Cloud Computing

Begünstigt durch Eigenschaften von Cloud-Infrastrukturen (u.a. die schnelle und einfache Verfügbarkeit neuer Ressourcen mit sehr guter Netzanbindung) ist die Nutzung von Cloud-Ressourcen für Angreifer sehr interessant, um beispielsweise Denial-of-Service (DoS) Angriffe auf andere Ziele durchzuführen oder Schadsoftware zu hosten.

Unsichere Schnittstellen und APIs

Cloud-Services und die von den Anbietern bereitgestellten Management-Schnittstellen sind bei Public-Cloud-Angeboten über das Internet erreichbar und können daher leicht angegriffen werden. Darüber hinaus stellen Cloud-Anbieter auch Programmierschnittstellen bereit, die von den Anwendern zur Steuerung und Konfiguration der Cloud-Services verwendet werden können. Schwachstellen in diesen Schnittstellen können ausgenutzt werden, um beispielsweise unrechtmäßigen Zugriff auf Kundendaten zu erhalten oder die dem Anwender zugeordneten Ressourcen missbräuchlich zu verwenden.

Böswillige Insider

Sicherheitsmaßnahmen der Software sind oft wirkungslos, wenn der Angreifer Zugriff auf die Infrastruktur des Cloud-Anbieters hat. Dies ist besonders bei böswilligen Insidern der Fall, also Mitarbeitern des Cloud-Anbieters, die sich Zugriff auf Kundendaten verschaffen. Hierzu zählen auch physische Angriffe im Rechenzentrum, wie z.B. der Diebstahl von Festplatten aus Servern, auf denen die Cloud-Services betrieben werden.

Risiken aufgrund mit anderen Cloud-Nutzern geteilten Technologien

Eine weitere Eigenschaft von Cloud Computing ist das sogenannte Pooling von Ressourcen. Dies bedeutet, dass die physischen Ressourcen von allen Anwendern der Cloud-Services verwendet werden. Dabei können sich z.B. Probleme bei der zuverlässigen Trennung der Nutzerdaten und -prozesse ergeben.

Datenverlust und Kompromittierung der Daten

Bei der Verwendung von Cloud-Services stellen sich aufgrund des Speicherorts der Daten in der Cloud als auch der Tatsache, dass viele unter Umständen nicht vertrauenswürdige Anwender gleichzeitig die Cloud-Infrastruktur verwenden, besondere Anforderungen an die Datensicherheit. Probleme bei Cloud-Providern in der Vergangenheit zeigten, dass es auch durch technische Probleme zu Datenverlusten kommen kann.

Diebstahl von Benutzerkonten oder Cloud-Diensten

Um die problemlose und angenehme Nutzung von Cloud-Diensten zu gewährleisten, setzen viele Cloud-Anbieter auf einen einfachen und schnellen Anmeldeprozess. Gelingt einem Angreifer, die Zugangsdaten eines Kundenkontos zu erlangen, kann er mit den Rechten dieses Kunden auf Daten zugreifen, Ressourcen missbräuchlich verwenden und Schaden anrichten.

Unbekannte (neue) Risiken

Um die Risiken von Cloud-Services abzuschätzen, müssen potentielle Anwender die Sicherheitsvorkehrungen und Maßnahmen der Anbieter analysieren und in die eigene Betrachtung mit einbeziehen. Wird eine solche Risikoanalyse nicht durchgeführt oder deckt sie nicht alle wichtigen Faktoren ab bzw. kann sie gar nicht erst durchgeführt werden, weil der Cloud-Provider die benötigten Informationen nicht bereitstellt, bleibt ein nicht einschätzbares Risiko bestehen.

Anforderungen an Cloud-Infrastrukturen

Eine wichtige Anforderung an eine Cloud-Infrastruktur ist eine solide Sicherheitsarchitektur sowie eine sichere Mandantentrennung auf allen Infrastrukturebenen (Virtualisierung, Netzwerk, Plattform, Anwendung, Daten). Weiterhin muss darauf geachtet werden, dass der Cloud-Provider nach einem definierten Vorgehensmodell für das Management von IT-Prozessen (z.B. ITIL, COBIT) arbeitet, um die vielen Aufgaben wie Patch-, Konfigurations-, Änderungs-, System- und Application-Management des Sicherheitsmanagements strukturiert anzugehen. Als Absicherung der Cloud gegen Störungen und Notfälle muss ein Notfallmanagement existieren. Zertifizierungen wie z.B. ISO 27001 können dem Anwender signalisieren, dass der Cloud-Anbieter solche Prozesse etabliert hat und gemäß diesen arbeitet.

Cloud-Nutzer sollten den Unternehmenshauptsitz des Cloud-Anbieters berücksichtigen; da viele bekannte Cloud-Anbieter ihren Unternehmenshauptsitz in den USA haben, unterliegen sie somit den dort geltenden Gesetzen wie z.B. dem Patriot Act, der US-Behörden Zugriff auf die Daten der Anwender erlaubt, ohne dass die Eigentümer der Daten darüber informiert werden. Dies gilt unabhängig davon, an welchem Ort die Cloud-Services betrieben und angeboten werden.

Die Frage nach der Nutzung von Cloud-Technologien und der Auslagerung von Diensten in die Cloud muss in erster Linie aus der Perspektive der Beherrschbarkeit mit den damit verbundenen Risiken betrachtet werden. Abhängig vom Einsatzszenario ergeben sich unterschiedliche Sicherheitsanforderungen. Diese werden in zahlreichen Studien und Leitfäden, wie z.B. von Fraunhofer AISEC[2], der BITKOM[3] [4], EuroCloud[5], ENISA[6], der CSA[7] sowie im Eckpunktepapier des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) „Sicherheitsempfehlungen für Cloud-Computing-Anbieter“[8] erläutert.

Sichere Nutzung von Cloud-Diensten

Folgende Maßnahmen sollte ein Anwender berücksichtigen, bevor er sich für die Nutzung eines Cloud-Services entscheidet und diesen tatsächlich im Unternehmen einsetzt:

Schutzniveau der Daten definieren
Bei der Erzeugung oder beim Transfer von Daten in die Cloud sollte der Anwender diese Daten klassifizieren (z.B. Sicherheitslevel „niedrig" bis „sehr hoch"), ihren Schutzbedarf analysieren und damit festlegen, welche Daten bei einem Cloud-Anbieter auf welche Weise gespeichert und übertragen werden dürfen. Dies kann beispielsweise die Verwendung bestimmter kryptografischer Verfahren oder ein umfassendes Rechtekonzept für den Zugriff auf bestimmte Informationen umfassen.

Sichere Speicherung der Daten in der Cloud
Bei der sicheren Speicherung der Daten spielt die Verschlüsselung eine zentrale Rolle. Bei allen Vorteilen durch Verschlüsselung ist die Verwaltung der Schlüssel eine Herausforderung, die dem Cloud-Anwender zufällt. Ein Verlust von Schlüsseln kann gleichzeitig den Verlust der damit verschlüsselten Daten bedeuten. Eine Kompromittierung der Schlüssel gefährdet direkt die Sicherheit dieser Daten.

Sicherer Transfer der Daten in die Cloud
Neben der sicheren und isolierten Aufbewahrung der Daten spielt der sichere Transport der Daten vom Kunden in die Cloud und zwischen den Rechenzentren der Cloud-Anbieter eine wichtige Rolle. Daten sollten nur über verschlüsselte Kanäle in die Cloud übertragen werden und können z.B. über ein verschlüsseltes virtuelles privates Netzwerk (VPN) in die bestehende IT-Infrastruktur des Anwenders eingebunden werden. Bei der Nutzung der Management-Schnittstellen oder von SaaS-Angeboten über den Web-Browser sollten nur verschlüsselte Verbindungen über HTTPS genutzt werden.

Sichere Datenverarbeitung
Bei der Datenverarbeitung ist es besonders wichtig, alle Zugriffe und alle Aktivitäten z.B. in den Speicherdiensten und Cloud-Anwendungen zu protokollieren und zu überwachen, um Angriffe frühzeitig zu erkennen. Des Weiteren spielen Portabilität der Daten und Interoperabilität der Cloud-Services eine wichtige Rolle, um die Gefahren eines Vendor-Lock-Ins, die zwangsweise Bindung an einen bestimmten Anbieter aufgrund fehlender Daten-Export-Schnittstellen oder wegen unüblicher Export-Datenformate, zu minimieren. Um einen Lock-In-Effekt zu vermeiden, müssen gegebenenfalls Vereinbarungen mit dem Cloud-Anbieter getroffen werden, um die in der Cloud gespeicherten Daten in einem Standardformat zur Verfügung gestellt zu bekommen, z.B. falls der Anwender das Angebot des bisherigen Cloud-Providers nicht mehr verwenden möchte oder im Fall des Bankrotts eines Cloud-Providers. Für die Integration von Cloud-Services in die eigene Infrastruktur bzw. bei der Nutzung mehrerer Cloud-Angebote (Hybrid Cloud) ist es wichtig, dass Cloud-Infrastrukturen interoperabel sind, was durch die Verwendung standardisierter und offener Schnittstellen, Protokolle und Open-Source-Plattformen erreicht werden kann.

Sicherer Zugang zu den Cloud-Diensten
Nicht nur die Daten selbst, die in der Cloud gespeichert und verarbeitet werden, sondern die Zugangsdaten der Anwender für den Cloud-Service müssen ebenfalls geschützt werden. Zugangsdaten sollten nur verschlüsselt übertragen und in regelmäßigen Abständen geändert werden. Dies auch unter dem Prinzip der Key-Rotation bekannt. Dabei sollten starke Authentifizierungsmechanismen wie eine Zwei-Faktor-Authentifizierung verwendet und Zugriffsrechte individuell nach dem Need-to-Know-Prinzip vergeben werden. Die vergebenen Rollen und Rechte müssen regelmäßig überprüft und aktualisiert werden.

Sichere Datenarchivierung
Die Datenarchivierung sollte ausschließlich verschlüsselt vorgenommen werden. Dabei müssen Mechanismen eingesetzt werden, die Suche und Extraktion von Daten zur Erfüllung regulatorischer Vorgaben und forensischer Untersuchungen jederzeit ermöglichen.

Sichere Datenlöschung/-vernichtung
Die dauerhafte Löschung ungenutzter Daten in der Cloud ist sehr wichtig, egal ob dies durch gesetzliche Vorgaben vorgeschrieben oder bei dem Wechsel des Cloud-Anbieters nötig geworden ist. Da ein Cloud-Anwender oft keinen direkten Zugriff auf das Backup durch den Cloud-Provider hat, bietet sich – sofern der Cloud-Service dies ermöglicht – an, Daten nur verschlüsselt in der Cloud zu speichern und beim Löschvorgang den entsprechenden Schlüssel zu vernichten, womit eine Entschlüsselung der Daten ausgeschlossen werden kann.

Fazit

Den Vorteilen der Nutzung von Cloud Computing (Skalierbarkeit, Elastizität, Pay-per-Use, ...) stehen einige Herausforderungen gegenüber, mit denen sich ein Anwender auseinandersetzen muss. Der Anwender muss überlegen, wie ihn Cloud-Infrastrukturen unterstützen können und welche Daten er in der Cloud verarbeiten möchte. Neben diesen und anderen oben angesprochenen Herausforderungen muss sich der Anwender bewusst sein, dass auch Cloud-Computing-Systeme zeitweise nicht erreichbar sein können und geeignete Strategien für Ausfallzeiten im Rahmen des Notfallmanagements entwickeln. Wird eine hohe Erreichbarkeit benötigt, besteht die Möglichkeit, mehrere unterschiedliche Clouds zu verwenden, was durch fehlende Schnittstellen aber in der Umsetzung schwierig sein kann.
Nichtsdestotrotz kann die Nutzung von Cloud-Infrastrukturen das Sicherheitsniveau von Anwendern, die im Bereich IT-Sicherheit und der sicheren Administration der eigenen Server wenig Expertise besitzen, sogar verbessern, da Cloud-Anbieter spezialisierte IT-Security-Mitarbeiter beschäftigen, die über aktuelle Angriffe frühzeitig informiert sind und die Systeme bei kritischen Schwachstellen zeitnah aktualisieren.

Dipl-Kffr., M.Sc. Iryna Windhorst
iryna.windhorst@aisec.fraunhofer.de

Dr. Niels Fallenbeck
niels.fallenback@aisec.fraunhofer.de

http://www.aisec.fraunhofer.de
http://www.cloud-competence-center.com

[1] Cloud Security Alliance: „Top Threats to Cloud Computing V1.0"; 2010.
[2] Werner Streitberger und Angelika Ruppel: „Cloud Computing Sicherheit – Schutzziele.Taxonomie.Markübersicht."; 2009
[3] BITKOM: „Cloud Computing – Evolution in der Technik, Revolution im Business"; 2009.
[4] BITKOM: „Cloud Computing – Was Entscheider wissen müssen"; 2010.
[5] EuroCloud: „Recht, Datenschutz & Compliance"; 2010.
[6] Catteddu, D. and Hogben, G., editors: "Cloud Computing Benefits, risks and recommendations for information security"; The European Network and Information Security Agency (ENISA), 2009.
[7] Brunette, G. and Mogull, R., editors: "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1"; Cloud Security Alliance, 2009.
[8] BSI Eckpunktepapier: „Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen in der Informationssicherheit"; 2012.