Sicherheitsaspekte des Cloud Computing

Rechtliches

Datenschutz und Rechtsstatus

Da sich die Daten innerhalb der Cloud physikalisch an einem beliebigen Punkt der Welt befinden und deshalb unter die entsprechende Rechtsordnung des Landes fallen könnten, ist es nahezu unmöglich, die Datenschutzbedingungen des Ausgangslandes(bei hohen Standards) einzuhalten.

Subunternehmer/Drittanbieter

Subunternehmer steigern ebenfalls die Undurchsichtigkeit für den Anwender, da die Daten nicht zwingend im Land des eigentlichen Anbieters gespeichert werden müssen.

Datenverlust

Datenverlust kann ebenfalls zu einem großen Problem innerhalb der Cloud führen, sollte Beispielsweise der Anbieter ein Insolvenzverfahren einleiten müssen.

Beschlagnahmung

Im Falle einer Beschlagnahmung von Hardware ist es ebenfalls möglich, dass die Daten des Anwenders(zumindest auf unbestimmte Zeit) verloren gehen.

Zugänglichkeit

Da Daten sich auf verteilten Systemen hin und her bewegen können und dadurch deutlich mehr Personal Zugriff auf die Daten hat, steigt die Wahrscheinlichkeit, dass Personen die gewillt sind, die Daten ungebührlich zu nutzen Zugriff auf diese erlangen.

Technisches

Keine Tools

Dadurch, dass es oftmals nicht möglich ist Sicherheits-, bzw. Kontrolltools auf den Systemen der Anbieter zu Installieren kann es schwierig sein, die Sicherheit der Anwendung zu überprüfen, bzw. zu überwachen.

Kein Zugriff auf Logs

Ist es nicht möglich alle Logs des Servers einzusehen kann dies die Erhöhungen und Kontrolle der Sicherheit ebenfalls schwierig gestalten, da nicht alle benötigten Informationen zur Verfügung stehen.

Datenverschlüsselung

Durch nicht existente oder unzureichende Verschlüsselung bei Übertragung oder Speicherung der Daten kann es möglich sein, dass Dritte Zugriff auf diese erhalten.

Suchmaschinen

Bei einigen Anbietern von Speicherdiensten ist es möglich, abgelegte Daten in Suchmaschinen zu finden und somit Ziele für potentielle Angriffe zu ermitteln.

Path Traversal

Der Anwender versucht hier durch ermitteln vorhandener Pfade und gezieltes Abändern selbiger Zugriff auf ungeschützte Ordner und Dateien zu erhalten.

XML Signature Wrapping Angriff

Durch Abfangen und Kluges Bearbeiten von SOAP Nachrichten kann der Angreifer Zugriff auf die Instanzen des Anwenders erlangen und diese nach Belieben manipulieren.

Cross Site Scripting

Hier werden Code-Injections genutzt um an die Anmeldedaten oder die Zertifikate der Nutzer zu gelangen.

SQL Injection

Sind die Datenbank des Anbieters oder deren Schnittstellen nicht ausreichend gesichert, kann dies Angreifern ermöglichen Zugriff auf sensible Daten zu erlangen oder diese sogar zu manipulieren bzw. löschen.

Remote File Inclusion

Mit Hilfe von RFI können Beispielsweise PHP Shells auf dem Server abgelegt werden. Der Server und die darauf befindlichen Daten werden somit kompromittiert.

Cross-VM Side-Channel Attacks

Es besteht die Möglichkeit andere, auf demselben Server befindliche VMs mit Hilfe der geteilten Hardware-Ressourcen zu attackieren.

Dadurch ist es beispielsweise möglich, Daten zu extrahieren und Tastenanschläge mitzuhören.

Literaturverzeichnis

Fraunhofer SIT. (2012). *SIT Technical Reports on the Security of Cloud Storage Services.* Stuttgart: Fraunhofer Verlag.

Juraj Somorovsky, M. H. (kein Datum). All Your Clouds are Belong to us - Security Analysis of Cloud Management Interfaces.

Martin Schweinoch, T. (2012. Mai 10). Die 10 größten Security-Risiken in der Cloud. *Computerwoche* .

Thomas Ristenpart, E. T. (kein Datum). Hey, Yout, Get Off of My Cloud: Exploring Information Leakage in Thrid-Party Compute Clouds.