CLOUD COMPUTING - SICHERHEIT IN DER WOLKE

Tobias Scheible

Mit Cloud Computing kann Rechenleistung, Speicherkapazität und Software in dem Umfang gemietet werden, wie sie tatsächlich benötigt wird. Damit können Unternehmen sich auf ihre Kerngeschäfte konzentrieren, ohne dass die IT zum limitierenden Faktor wird. Für den Einsatz entscheidend sind neben den Anforderungen von technischer Seite jedoch vor allem die Sicherheit, der Datenschutz und die Compliance Rahmenbedingungen. Dieser Artikel befasst sich vorrangig mit einer Erläuterung der grundlegenden Funktionsweise und anschließend intensiver mit dem komplexen Bereich „Sicherheit".

An einem Dokument mit einem über die ganze Welt verteilten Team arbeiten, mehrere Terrabyte Daten mit einem Smartphone verwalten oder ein ganzes Unternehmen mit einem Browser organisieren: das alles ist Cloud Computing.

Der Name Cloud Computing stammt von der Metapher „Wolke". Diese „Wolke" dient in Netzwerkdiagrammen zur Darstellung eines nicht näher spezifizierten Bereiches. Vereinfacht kann das Konzept wie folgt erläutert werden: anstatt eine eigene IT-Infrastruktur zu betreiben, greift man auf die Infrastruktur eines Cloud-Anbieters zurück und mietet sich die benötigten Ressourcen. Durch dieses Vorgehen sind IT-Leistungen und Ressourcen quasi überall verfügbar, da sie als Service über das Internet bezogen werden. Der Vorteil für Unternehmen liegt in einer deutlichen Kostenersparnis und einer verbesserten Flexibilität. Gerade kleine und mittlere Unternehmen können auf diese Weise innovative Leistungen in einer beliebigen Anzahl in Anspruch nehmen, ohne in den Aufbau und das Personal für die Wartung von großen Rechenzentren zu investieren.

Bill Gates ahnte bereits 2005 die Entwicklung des Cloud Computings voraus und wies seine Mitarbeiter in einer Rundmail auf die Chancen und Gefahren dieser Entwicklung in der IT-Branche hin. Mit den Worten „Der nächste grundlegende Wandel steht uns bevor" beschrieb er die Veränderung. „Die breite und reichhaltige Basis des Internets wird eine ‚Service -Welle' von Anwendungen und Erfahrungen lostreten, die sofort zur Verfügung stehen werden", so Gates weiter. Mit dem Satz „Diese neue Welle wird sehr disruptiv sein." machte er allen klar, wie ernst die Lage ist und welche Anstrengungen Microsoft aufbringen muss, um diesen Wandel erfolgreich zu meistern [1].

Immer größer und effizienter werdende Rechenzentren werden die Preise für Cloud Computing in Zukunft immer weiter sinken lassen. Dadurch wird es für Unternehmen immer unattraktiver eine eigene Infrastruktur aufzubauen [2]. Sobald ein Unternehmen jedoch seine IT-Leistung aus einer Cloud bezieht, kann sich dadurch ein Wettbewerbsvorteil ergeben, da die Konkurrenz eine ähnliche Kostenreduktion erreichen muss, um langfristig im Markt zu bestehen.

Heutzutage können Unternehmen bereits ihre Lizenz- und Wartungskosten reduzieren, indem sie auf reine Software as a Service, kurz SaaS-Lösungen setzen. Der mobile Bereich hat außerdem das Cloud Computing beflügelt. Es stehen immer mehr Endgeräte in Form von Smartphones und Tablets zur

Verfügung und diese werden von immer mehr Menschen genutzt. Diese mobilen Endgeräte sind vergleichsweise rechenschwach und nutzen Cloud Services mithilfe der installierten Apps.

Cloud-Beispiel Google Drive

Eines der bekanntesten Beispiele für die Verwendung von Cloud Computing ist die webbasierte Office-Anwendung Google Drive (früher mit Google Docs und in Deutschland mit Google Text & Tabellen bezeichnet). Die Dokumente werden hierbei unabhängig vom Standort der Benutzer irgendwo in den Rechenzentren des Suchmaschinen-Giganten gespeichert. Die Bedienung der Office Anwendung erfolgt über einen Webbrowser. Die Berechnungen in der Tabellenkalkulation werden in riesigen Server-Farmen durchgeführt und dem Benutzer wird nur das Ergebnis ausgegeben. Die eigentlichen Rechenvorgänge bleiben für den Benutzer in der Cloud verborgen.
Durch dieses Vorgehen steht jedem Nutzer eine Office-Anwendung zur Verfügung, die nicht installiert werden muss und die jederzeit und überall auf alle gespeicherten Dokumente zugreifen kann. Die minimale Anforderung zur Nutzung dieses Dienstes ist ein Rechner mit einem Webbrowser und ein Internetzugang. Weitere bekannte Beispiele für Cloud-Anwendungen sind Dropbox, Flickr und iCloud.

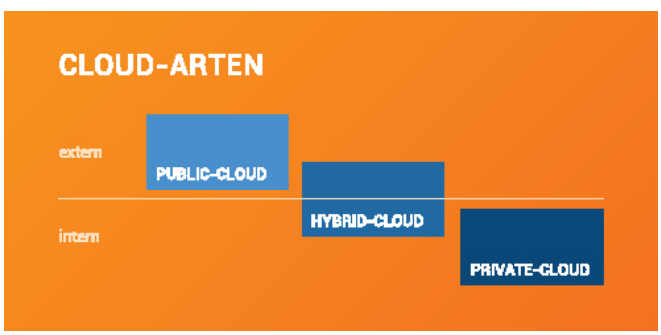
Der Weg zur Cloud

Bisher dominierten grundsätzlich zwei Modelle die Datenverarbeitung. Die Verarbeitung von Daten mit Großrechnern in Rechenzentren ist dabei die älteste Variante. Hier wurden die Berechnungen zentral von speziellem Personal durchgeführt. Diese Systeme kamen hauptsächlich in der Wissenschaft und in großen Verwaltungen zum Einsatz. Das nächste Modell ist die Client-Server-Architektur, bei der mehrere Rechner über einen Server miteinander verbunden sind. Hierbei greifen zum Beispiel mehrere Clients auf eine zentrale Datenbank im lokalen Netzwerk zu [3]. Als weiterer Entwicklungsschritt ist nun das Cloud Computing dazugekommen. Anwendungen werden nicht mehr lokal ausgeführt und Daten nicht mehr lokal gespeichert. Sowohl die Ausführung der Anwendung als auch die Speicherung der Daten wird auf externe Infrastrukturen ausgelagert. Die dafür verwendeten Technologien sind nicht neu, aber deren Nutzung beschreitet einen neuen Weg. Zum Beispiel verwenden Webanwendungen ähnliche Prinzipien wie sie beim Cloud Computing Einsatz finden und stellen dem Nutzer verborgene Leistung zur Verfügung.
Allerdings agiert Cloud Computing nicht nur im Bereich von Anwendungen, sondern vor allem auch auf der Ebene von Daten und Rechenleistung. So betreibt zum Beispiel Dropbox eigene Server für die Website und die Verwaltung der Benutzer, benutzt aber für die Speicherung der großen Datenmengen den Cloud-Service S3 von Amazon.

Geschwindigkeit für die Cloud

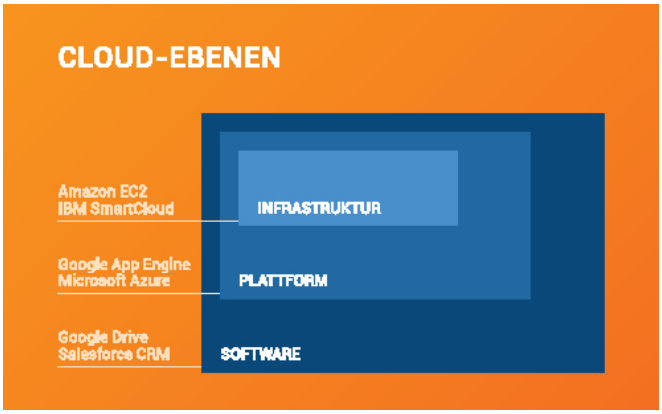
Erst die Weiterentwicklung und Ausbau der Internetbandbreite ermöglichte die Entwicklung und Nutzung von Cloud Computing. Umso größer die Geschwindigkeit, desto komplexere Leistungen können über das Internet angeboten werden. Der ehemalige CEO von Google, Eric Schmid, hatte schon 1993 während seiner Zeit bei SUN diese Entwicklung beschrieben: „Wenn das Netzwerk so schnell wie der Prozessor wird, wird der Computer ausgehöhlt und über das Netzwerk verteilt." Ende der 90er-Jahre erfolgte mit dem Dotcom-Boom der großflächige Ausbau der Netzbandbreite. Modems wurden immer schneller und der ISDN-Anschluss wurde eingeführt [4]. Die Rechenzentren wurden untereinander mit Glasfaserverbindungen vernetzt und die gesamte Netzwerkinfrastruktur wurde immer schneller. Nach der Jahrtausendwende etablierte sich der DSL-Breitbandanschluss immer mehr und machte so eine schnelle Verbindung in vielen Bereichen verfügbar. Mittlerweile sind bis zu 100 MBit/s Internetanschlüsse über das Fernsehkabel verfügbar und haben damit die lokale Netzwerkgeschwindigkeit erreicht, die noch vor ein paar Jahren Standard war. Der nächste Schritt in der globalen Vernetzung ist der Glasfaseranschluss für private Nutzer. Die Telekom hat mittlerweile die Liste mit Städten veröffentlicht, in denen das Fiber-To-The-Home-Netz mit einer Geschwindigkeit von 200 MBit/s im Downstream und 100 MBit/s im Upstream starten wird [5]. Und Google hat selbst in den USA ein Glasfaser-Angebot mit einer Geschwindigkeit von 1 GBit/s gestartet [6]. In London startet der britische Kabelnetzbetreiber Virgin Media einen Versuch für Anschlüsse mit einer Übertragungsrate von 1,5 GBit/s [7]. Damit hat die Geschwindigkeit des Internets eine Schwelle erreicht mit der sie mit lokalen Netzwerken gleichziehen kann.

Arten von Clouds



Grundsätzlich kann Cloud Computing in zwei Bereiche unterteilt werden: Public und Private Clouds [8]. Public Clouds werden von externen Anbietern betrieben und von vielen Benutzern in Anspruch genommen. Zum Beispiel laufen auf der Cloud-Platform Windows Azure mehrere Instanzen von unterschiedlichen Kunden. Private Clouds werden von einem Unternehmen betrieben und stellen eine Inhouse-Lösung dar. Ein bekanntes Beispiel dafür ist die Dropbox Alternative ownCloud, die auf einem eigenen Webserver installiert werden kann. Eine Mischform aus diesen beiden Formen stellt die Hybrid Cloud dar. Hierbei betreibt ein Unternehmen eine Private Cloud und nutzt eine Public Cloud als Backup-Lösung oder um Lastspitzen abzufangen. So können mehrere QNAP-NAS-Systeme zu einer lokalen Private Cloud miteinander verknüpft werden und es kann über den Public Cloud Anbieter ElephantDrive ein Backup erstellt werden. Eine Sonderform stellt die Community Cloud dar. Hier schließen sich mehrere Unternehmen zusammen und nutzen gemeinsam eine Private Cloud.

Ebenen von Clouds



Es wird zwischen drei Ebenen bei Cloud Computing unterschieden [9]. Die erste Ebene repräsentiert die Infrastruktur (IaaS - Infrastructure as a Service). Hier werden zum Beispiel Dateien gespeichert und es wird auf Datenbanken zugegriffen. Unter dem Namen Amazon Web Services stellt Amazon mehrere Cloud-Dienste bereit. So können mit dem Service Elastic Compute Cloud (EC2) von Amazon virtuelle Host erstellt werden, die in der Cloud von Amazon betrieben werden. Ein weiterer Anbieter auf der Infrastruktur Ebene ist zum Beispiel IBM mit der SmartCloud.
In der nächsten Ebene, die als PaaS - Platform as a Service bezeichnet wird, werden Programme direkt ausgeführt. Hier kann zum Beispiel die Google App Engine oder Windows Azure genutzt werden, um schnell eine Entwicklungsumgebung aufzusetzen oder beliebig skalierbare Leistungen für eine Produktivversion abzurufen.
Die letzte Ebene der Cloud ist die Software selbst. Hier wird dem Benutzer das Interface als Service bereitgestellt. Dieses Prinzip wird als Software as a Service bezeichnet. Das prominenteste Beispiel hierfür ist die oben bereits erwähnte Office Anwendung Google Drive.
Die unterschiedlichen Ebenen der Cloud lassen sich beliebig miteinander kombinieren und auch mit Nicht-Cloud-Anteilen verknüpfen, sodass eine scharfe Abgrenzung der „Wolke“ nahezu unmöglich ist. Laut Definition ist jedoch grundsätzlich von Cloud Computing die Rede, sobald Ressourcen flexibel über das Internet zugeteilt werden können.
Die Spannbereite reicht dabei wie bereits erläutert über mehrere Ebenen hinweg von einfacher Rechenleistung, über Speicherkapazität bis hin zu Software. Im Vergleich zur klassischen IT-Outsourcing stehen bei Cloud Computing die schnellere Flexibilität und die Grundprinzipien „Nutzung nach Bedarf“ und „Bezahlung nach Nutzung“ im Vordergrund.
Oftmals wird das Webhosting ebenfalls als Cloud bezeichnet. Streng genommen handelt es sich an dieser Stelle aber nicht um Cloud Computing, da sich die benötigten Ressourcen normalerweise auf einem Server befinden.

VORTEILE

Cloud Computing ist der nächste Schritt in der Evolution der Informationstechnologie, allerdings ist es mehr als ein reines IT- oder das Technologie-Management Thema. Denn durch die stärkere Unabhängigkeit von Geschäftsprozessen und den IT-Ressourcen sind Unternehmen flexibler und können schneller Innovation hervor bringen [10 S.20, 11 S.8].

Einfachheit

Bei vielen Cloud Diensten kann man sich online anmelden und die Dienste direkt danach nutzen. Viele Dienste, wie die Online-CRM Anwendungen von Salesforce, abstrahieren komplexe Prozesse für die Benutzer. So kann eine komplexe Anwendung die auf vielen Servern läuft einfach über ein Webinterface bedient werden.

Kostenersparnis

Bei Cloud Computing können schnell Ressourcen gebucht werden, die im Moment benötigt werden. Gerade durch die „Bezahlung nach Nutzung“ müssen Ressourcen nicht gezahlt werden die normalerweise nur zur Sicherheit vorgehalten werden müssen. So nutzt das Online-Empfehlungsportal Qype die Google Apps für die Nutzung von E-Mails und Kalendern. Damit musste keine eigene kostenintensive Mail-Server-Infrastruktur installiert und gepflegt werden.

Skalierbarkeit

Kleine Unternehmen müssen keine Infrastruktur aufbauen, sondern nutzen die Dienste der Cloud. Und damit können sie benötigte Ressourcen je nach Bedarf buchen. Flickr, die Plattform für den Austausch von Fotos, speichert beispielsweise alle Daten in der Cloud von Amazon. So konnten sich die Entwickler auf die Programmierung des Systems konzentrieren und Flickr konnte kontinuierlich wachsen, ohne dass es einen Engpass bei der Speicherkapazität gab.

Zukunftssicherheit

Der Vorteil bei Cloud Computing ist, dass sich Spezialisten in großen Rechenzentren um tausende einzelner Rechner kümmern. Durch den Charakter von Cloud-Angebote können einzelne Rechner ausgetauscht werden ohne dass der Betrieb beeinträchtigt wird. Damit lassen sich während des Betriebs Hardware-Komponenten austauschen und Software aktualisieren. Damit regeneriert sich die Cloud von selbst und ist immer auf dem neuesten Stand. So nutzt man bei der Online-Office Variante von Microsoft Office 365 immer die neuesten Versionen.

Nachhaltigkeit

Green-IT ist in letzter Zeit eines der Hype-Themen und auch bei Cloud-Computing kommt es zum Zuge. So können große zentrale Rechenzentren effizienter betrieben werden als viele kleine lokale Zentren, da deren Auslastung konstanter ist. In kleinen Zentren liegen zur Pufferung von Lastspitzen jedoch oft viele Ressourcen brach. Amazon nutzt diesen Aspekt für die eigenen Rechenzentren und die Cloud Angebote geschickt aus. So greifen in der Vorweihnachtszeit sehr viele Benutzer auf Amazon zu, und es wird mehr Leistung als sonst für die eigene Website benötigt. Im Gegenzug befinden sich aber viele Mitarbeiter des Unternehmens im Urlaub und somit werden die Cloud-Dienste nicht so stark wie normal genutzt.

NACHTEILE

Den Vorteilen stehen natürlich auch einige Nachteile gegenüber. Die grundlegende Eigenschaft der Cloud, dass Daten “irgendwo” gespeichert werden, kann schnell zu einem Nachteil werden. So werden geschäftsinterne Daten und das Know-how des Unternehmens extern gespeichert und verwaltet [10 S.20, 11 S.8].

Abhängigkeit

Werden Geschäftsprozesse in die Cloud verlagert, begibt sich ein Unternehmen in eine starke Abhängigkeit vom jeweiligen Anbieter. Geht dieser Anbieter insolvent oder muss aus anderen Gründen den Geschäftsbetrieb einstellen, steht es schlecht um die Kundendaten. Oftmals besteht keine Chance, auf die Rohdaten direkt zuzugreifen. Außerdem können diese Daten oft ohne die passende Software nicht mehr weiterverwendet werden.

Internetzugang

Da auf viele Dienste über das Internet zugegriffen wird, entstehen zusätzliche Abhängigkeiten. Besteht keine Internetverbindung zum Anbieter, ist kein Arbeiten mehr möglich. Es kann an einer Unterbrechung des eigenen Internetanschlusses liegen oder an einer Unterbrechung im jeweiligen Rechenzentrum. Da die benötigte Netzwerkinfrastruktur deutlich komplexer ist als beim lokalen Betrieb, erhöht sich das Risiko einer Unterbrechung.

Verwaltung

Dabei spielen auch Einflussfaktoren eine Rolle, die nicht auf den ersten Blick offensichtlich sind. So ist es dem Internet-Start-Up Radio.de ergangen. 48 Stunden war das Unternehmen lahmgelegt. Es konnten weder E-Mails versendet oder empfangen werden noch konnten interne Dokumente geöffnet werden. Und das an beiden Standorten, in Hamburg und Innsbruck, obwohl die Netzwerkinfrastruktur in Ordnung war. Der Grund für diesen Blackout war ein Fehler in der Abrechnung. Radio.de nutzt für die Büroanwendungen die Dienste von Google. Durch einen Fehler im Bezahlsystem konnte sich kein Mitarbeiter mehr einloggen [12].

Verlässlichkeit

Die Zentralisierung hat auch dazu geführt, dass mehrere Unternehmen von einem Anbieter abhängig sind. So hat eine Störung bei Amazon dafür gesorgt, dass die bekannten Dienste Foursquare, Quora und Reddit gleichzeitig mit Störungen zu kämpfen hatten. Diese Störung war so gravierend, dass Daten unwiederbringlich verloren gegangen sind.

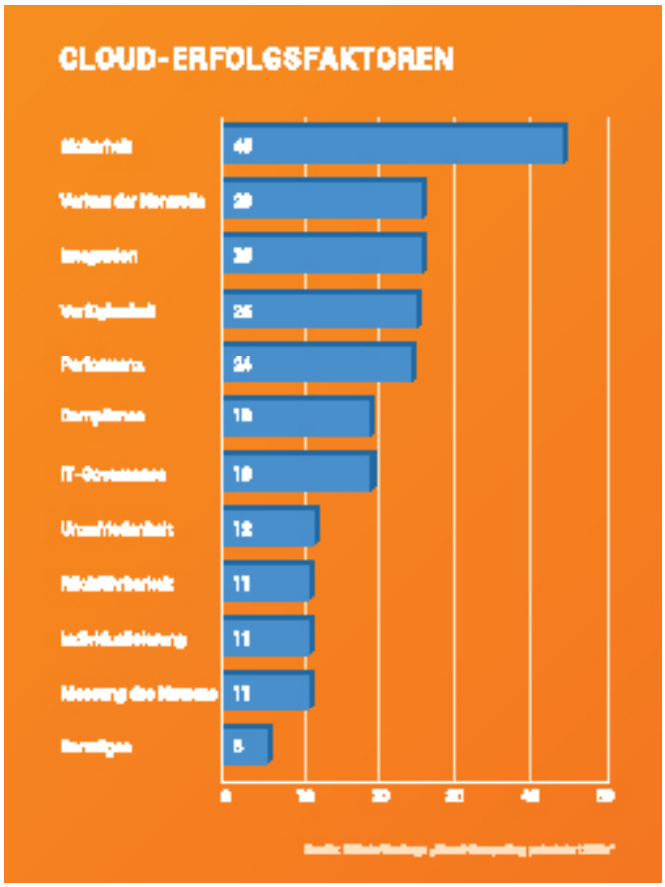
Interoperabilität

Der Wechsel eines Cloud-Anbieters ist nicht ohne weiteres möglich, da ein automatischer Umzug nicht vorgesehen ist und die Anbieter untereinander inkompatibel sind. Mittlerweile gibt es zwar erste Ansätze für die Entwicklung von Standards im Cloud Computing, um beispielsweise Daten zwischen Anbietern auszutauschen und somit einen Wechsel des Anbieters vorzunehmen. Jedoch braucht diese Entwicklung noch einige Zeit um sich als Standard zu etablieren.

Sicherheit & Datenschutz

Die beiden Punkte Sicherheit und Datenschutz stellen zusammen die größten Nachteile im Vergleich mit anderen Infrastrukturen dar und damit die größten Hürden für die Verwendung von Cloud Computing. Im Nachfolgenden werden diese beiden Punkte genauer betrachtet.

SICHERHEIT UND CLOUD COMPUTING



Die Sicherheitsmaßnahmen beim Cloud Computing unterscheiden sich nicht grundlegend von den Sicherheitsmaßnahmen bei herkömmlichen IT-Infrastrukturen. Anforderungen, Bedrohungen, Richtlinien und Kontrollen sowie Governance und Compliance sind größtenteils identisch [13 S.4].
Aufgrund der Unterschiede in der gemeinsamen Nutzung, Teilung, Kontrolle und Verwaltung von Ressourcen sind jedoch einige Anpassungen und andere Gewichtungen notwendig. Gerade durch den typischen Charakter von Cloud Computing kann es zu Schwachstellen kommen, da viele Schnittstellen benutzt werden und die Daten auf viele Server oder sogar Anbieter verteilt sind. Dieses System bietet neben den oben genannten Vorteilen auch die Gefahr einer Vielzahl von Angriffspunkten.
Für einen besseren Überblick werden die verschiedenen Angriffsarten in Kategorien unterteilt. So kann von passiven und aktiven sowie von externen und internen Angriffen gesprochen werden [11 S.12].

passive Angriffe

Bei einem passiven Angriff findet kein Eingriff in das Cloud -System statt. Meist erfolgt der Angriff durch das Abfangen der Kommunikation zwischen einem Benutzer und der Cloud. Da durch dieses Vorgehen keine Veränderung am System vollzogen wird, sind diese Angriffe nur sehr schwer zu erkennen. Ein typisches Beispiel für ein derartiges Szenario ist ein Man-in-the-middle-Angriff. Schutz gegen diese Art von Angriffen bietet nur eine durchgängige Verschlüsselung, wobei der Schlüssel außerhalb der Cloud auf einem alternativen Weg ausgehandelt werden sollte.

aktive Angriffe
Bei einem aktiven Angriff greift der Angreifer direkt auf das System zu. Dabei werden zum Beispiel Sicherheitslücken ausgenutzt oder Passwörter per Brut-Force geknackt. Bei dieser Art von Angriff hinterlässt der Angreifer Spuren, durch die der Angriff erkannt und mit denen der Angreifer im besten Fall identifiziert werden kann.

externe Angriffe
Hier wird das Cloud-System von einer unbeteiligten Person von außerhalb angegriffen. Dabei kann man zwischen Hackern, Crackern und Script-Kiddies unterscheiden. Diese unterscheiden sich nach Erfahrungslevel und Motivation. Hacker haben meist ausgeprägt Kenntnisse und versuchen Sicherheitsmechanismen der Systeme zu überwinden. Ihre Motivation ist es mit ihren Fähigkeiten Schwachstellen aufzuzeigen und nicht Systeme anzugreifen. Cracker hingegen haben meist das gleiche Wissensniveau, allerdings handeln sie aus kommerziellen Interessen oder aus emotionalen Gründen, wie zum Beispiel um Rache zu nehmen. Oft erfolgen auch Angriffe um ein System zu kapern und von diesem aus einen verschleierten oder größeren Angriff zu starten. Cracker werden beispielsweise auch von Konkurrenten beauftragt um System zu sabotieren oder Informationen zu stehlen. Script-Kiddies haben dagegen oftmals keine tieferen IT-Fähigkeiten und führen Angriffe mit fertigen Skripten durch. Häufig kennen sie die verwendeten Funktionen nicht und sind sich der Konsequenzen ihre Handlungen nicht bewusst.

interne Angriffe
Neben den Angriffen von außerhalb, spielen Angriffe aus dem Nutzerfeld, also von internen Personen mit Bezug zum Unternehmen eine zunehmende Rolle. Zu den potentiellen internen Angreifern gehören neben den (ehemaligen) Mitarbeitern auch Praktikanten, externe Mitarbeiter, Kooperationspartner und Mitarbeiter des Cloud-Anbieters oder auch andere Kunden des Cloud-Anbieters.

GEFAHREN BEIM CLOUD COMPUTING

Zugangsdaten
Durch die zentrale Verwaltung der Leistungen bei Cloud Anbietern können Angreifer durch den Diebstahl von Zugangsdaten oft auf mehrere Systeme gleichzeitig zugreifen. Neben den üblichen Methoden um Zugangsdaten zu schützen, müssen für diese kritischen Bereiche noch weitere Maßnahmen ergriffen werden. Eine automatische Benachrichtigung des Administrators bei einer Aktivität (Login, Änderung, ...) oder eine Zwei-Wege-Authentifizierung können hier die Sicherheit deutlich erhöhen.

Zugriffsrechte
Mitarbeiter mit kriminellen Absichten stellen für jedes Unternehmen eine potentielle Gefahr dar. Bei Cloud Computing kommen jedoch noch die Mitarbeiter des Anbieters zusätzlich hinzu, die nicht den unternehmenseigenen Richtlinien unterliegen. Um hier die Gefahr zu verringern, sollten mehrere Ebenen von Zugriffsrechten eingerichtet werden, damit jede Person nur auf die wirklich notwendigen Bereiche zugreifen kann. Des Weiteren sollten alle Zugriffe protokolliert werden - das Protokoll sollte somit auch die Mitarbeiter der Cloud-Anbieter beinhalten. Hier ist es ebenfalls empfehlenswert eine Benachrichtigungsfunktion einzurichten.

Schnittstellen
Der Zugriff auf viele Cloud-Dienste erfolgt über offen protokollierte Schnittstellen. Um hier die Sicherheit zu erhöhen sollten alle Zugriffe verschlüsselt erfolgen und mit entsprechend starken Authentifizierungs-Methoden abgesichert werden. Des Weiteren sollten zudem alle Zugriffe protokolliert werden um potentielle Angriffe zu erkennen.

Geteilte Ressourcen
Durch die flexible Skalierbarkeit werden die Daten in viele Cloud-Rechenzentren auf mehreren Systemen verteilt und mit andern Kunden gemeinsam genutzt Immer wieder gibt es Meldungen, dass es Angreifern gelungen ist aus virtuellen Maschinen auszubrechen und somit die Möglichkeit besteht andere virtuelle Instanzen auf demselben Host anzugreifen. Daher müssen Anbieter Techniken einsetzen, um die einzelnen Kundenbereiche klar voneinander abzugrenzen und dafür Sorge tragen, dass kein Ausbruch aus einer virtuellen Maschine möglich ist.

Verschlüsselung
Oftmals werden von den Cloud-Anbietern keine konkreten Informationen veröffentlicht welche Verschlüsselungs-Algorithmen sie einsetzen. Außerdem gibt es einige Anbieter, bei denen die Übertragung (noch) komplett unverschlüsselt stattfindet. Auch allgemeine Verschlüsselungen bei denen ein Anbieter alle Daten von allen Kunden mit demselben Passwort verschlüsselt, sollten als unsicher angesehen werden. Alle Übertragungen und Verbindungen müssen verschlüsselt erfolgen, sobald unternehmenskritische oder Datenschutz relevante Daten in der Cloud gespeichert werden, sollten diese mit einem individuellen Passwort ergänzt werden, welches dem Cloud-Anbieter nicht bekannt ist.

Datenlokalität
Der Vorteil der Cloud ist, dass die Ressourcen beliebig skaliert werden können und von überall aus abgerufen werden können. Aber nicht alle Anbieter legen offen in welchem Land die Daten gespeichert werden. So kann es zu datenschutzrechtlichen Problemen kommen, wenn beispielsweise personenbezogene Daten außerhalb der EU gespeichert werden. Diese sollten mit dem Cloud-Anbieter vertraglich geregelt werden in welchem Land die Daten gespeichert werden.

Sicherheitsvorfälle
Da bei Cloud-Umgebungen die Angriffe auch über die Cloud-Infrastruktur selbst erfolgen können, muss der Anbieter gegen diese Art von Angriffen eine Strategie ausgearbeitet

haben. Dazu gehört unter anderem, dass im Zweifelsfall erfolgreiche Angriffe den entsprechenden Kunden gemeldet werden und diese damit entsprechende Maßnahmen, wie zum Beispiel die Änderung aller Passwörter, ergreifen können. Da Kunden in Cloud-Umgebungen jedoch nicht auf alle Ebenen eines Systems zugreifen können, haben die Cloud-Anbieter die Aufgabe relevante Daten für eine Ermittlung zu erheben und zu sichern. Zur Erfüllung dieser Aufgabe muss der Anbieter vertraglich verpflichtet werden entsprechende Beweise zu sichern.

Kündigung

Nachdem ein Vertrag mit einem Cloud-Anbieter gekündigt wurde, müssen alle Daten vollständig gelöscht werden. Da sich auch hier wieder mehrere Kunden die Infrastruktur teilen und Ressourcen wieder schnelll freigegeben werden können, muss das Löschen sicher erfolgen. Es muss darauf geachtet werden, dass vertraglich vereinbart wird, wann und wie die verbleibenden Daten von einem Cloud-Anbieter gelöscht werden. Wichtig dabei ist, dass diese Regelungen sich auch auf alle Duplikationen und Backups beziehen müssen.

Missbrauch

Cloud-Infrastrukturen können allerdings auch für Angriffe genutzt bzw. missbraucht werden. So hat der deutsche Hacker Thomas Roth mit Hilfe geclusterten GPU-Instanzen SHA1 verschlüsselte Passwörter der NSA dechiffriert [14]. Dabei erwies sich die Miete für den Cloud-Dienst günstiger als die Kosten für die Nutzung eines illegalen Botnetzes. Der Missbrauch einer Cloud-Infrastruktur wird dadurch begünstigt, dass es bei einigen Cloud-Anbieter möglich ist sich anonym, d.h. nur durch die Angabe einer Kreditkarte zu registrieren.Es wäre wünschenswert, dass alle Cloud-Anbieter die Identität einer Person besser überprüfen um illegale Aktivitäten zu unterbinden.

DER KONFLIKT MIT DEM DATENSCHUTZ

Einer der noch nicht vollständig geklärten Aspekte ist der datenschutzkonforme Umgang mit den Daten in der Cloud, wobei sich der Begriff „Datenschutz“ im deutschen Recht im Wesentlichen auf personenbezogene Daten bezieht. Wenn die Daten auf Servern in verschiedenen Ländern verteilt werden, unterliegen diese auch den jeweiligen landestypischen Gesetzen. Somit wird einer der größten Vorteile des Cloud Computings, die hohe Abstraktion, zu einem Problem. Daher muss bei der Auswahl des Anbieters darauf geachtet werden, in welchen Ländern und damit nach welchen Gesetzen die Daten gespeichert werden [15]. Es kommt zum Beispiel zu Problemen, wenn personenbezogene Daten außerhalb der Europäischen Union gespeichert werden. Die außereuropäischen Länder gelten als datenschutzrechtlich kritisch bzw. unsicher [16]. Als Ausnahme ist hier die USA zu sehen, da zwischen der USA und der EU eine Safe-Harbor-Vereinbarung existiert [17].
Neben personenbezogenen Daten unterliegen jedoch auch andere Dokumente rechtlichen Vorschriften, so müssen beispielsweise steuerlich relevante Dokumente grundsätzlich im Inland aufbewahrt bzw. archiviert werden. Das gleiche gilt, gemäß des deutschen Handelsrechts auch für Buchungsbelege und Handelsbriefe. Der Tatsache, dass die Unternehmen, die die persönlichen Daten erheben für die Sicherheit und den Datenschutz verantwortlich sind und nicht der Cloud Computing-Anbieter sind zu beachten [18]. Wichtig ist auch zu berücksichtigen, dass viele Cloud-Anbieter selbst ein Subunternehmen beauftragen. So werden die Daten von Dropbox in der Cloud von Amazon gespeichert, wodurch die Daten den Regelungen von Amazon unterliegen. Gerade diese Unsicherheit macht eine eigene private EU-Cloud für Unternehmen interessant.
Eines der Hauptprobleme ist, dass die Cloud-Anbieter nicht alle Schritte und Maßnahmen offenlegen. So wird in der Regel nicht veröffentlicht welche Prozesse angewandt werden um Daten vor unbefugten Zugriffen zu schützen. Die fehlende Transparenz in diesem Bereich verhindert heutzutage noch den breiten Einsatz von Cloud-Computing.

DAS PROBLEM DER TRANSPARENZ

Oftmals praktizieren heutige Anbieter Sicherheit durch Verschleierung, allerdings kann ein hoher Sicherheitlevel nur mit Transparenz erreicht werden [11 S. 29]. Solange die Anbieter nicht offenlegen, wie die Daten und System gesichert sind und wo sich die dazugehörigen Infrastrukturen befinden, ist kein Vergleich und vor allem keine Kontrolle über die eigenen Dienste und Daten möglich [19 S.9]. Aber vor allem ist dadurch nicht klar wer theoretischen Zugriff hat, und welche Maßnahmen zur Sicherung angewendet werden. Durch die fehlenden Informationen können deshalb Public Clouds nicht datenschutzkonform genutzt werden. Außerdem stehen sie oftmals auch im Widerspruch zu vorhandenen IT-Compliance Regeln. Ein dokumentiertes Datenschutzmanagement und ein veröffentlichtes IT-Sicherheitsmanagement Konzept ist derzeit leider noch bei fast keinem Anbieter anzutreffen.
Ein Ansatz um für mehr Transparenz zu sorgen ist die Einführung von Cloud Compliance um die nachweisbare Einhaltung von unternehmensinternen und vertraglichen Regelungen zur Nutzung oder Bereitstellung von Cloud Computing Leistungen zu garantieren. Damit kann Cloud Compliance die bestehende Zurückhaltung und die Vorbehalte gegenüber den Angeboten zum Cloud Computing reduzieren. Allerdings müssen dabei die beiden Herausforderungen der Neuartigkeit und der Komplexität bewältigt werden. Dadurch dass unterschiedliche Anbieter auf Grund ihrer unterschiedlichen Leistungen nicht verglichen werden können, müssen jeweils individuelle Vereinbarungen getroffen werden. Allerdings können die Cloud-Compliance Regelungen auf den klassischen und bereits vorhandenen IT-Compliance-Anforderungen aufbauen, da es sich ja um eine neue Nutzungsmethode handelt und nicht um eine neue Technik. Duch dieses Vorgehen sollten also die klassischen IT-Risiken wie Sicherheit, Verfügbarkeit, Vollständigkeit und Nachvollziehbarkeit bereits abgedeckt sein.

ZUSAMMENFASSUNG

Cloud Computing hat die IT-Branche stark verändert und wird die zukünftige Entwicklung noch weiter stark beeinflussen. Ein oft gezogener Vergleich ist die Entwicklung in der Stromwirtschaft am Ende des 19. Jahrhunderts. Damals erfolgte eine Umstellung von vielen kleinen Stromerzeugern hin zu einem landesweiten Stromnetz mit zentralen Großkraftwerken. Dasselbe geschieht nun gerade in der IT-Branche. Ressourcen wie Speicherplatz und Rechenleistung werden von Cloud-Anbietern in großen Rechenzentren bereitgestellt. Dieser Prozess fördert eine Art Demokratisierung der IT-Branche. Ein kleines Start-Up kann per Cloud mit einem globalen Unternehmen konkurrieren, ohne eine eigene Infrastruktur aufbauen zu müssen. Zudem treibt die schnelle Entwicklung bei den mobilen Plattformen die Weiterentwicklung zusätzlich flott voran. Durch diese Entwicklung verschieben sich auch die Sicherheitsmaßnahmen weg von einzelnen Rechner und Server bis hin zu zentralen Systemen.

Cloud Computing unterliegt grundsätzlich den gleichen Angriffsgefahren wie eine traditionelle Infrastruktur. Allerdings steigt die Gefahr eines Angriffs durch die Vereinfachung und Zentralisierung. So kann zum Beispiel ein Angreifer durch das Ausspähen von Zugangsdaten Zugriff auf eine komplette Infrastruktur mit mehreren Servern bekommen. Durch diese Komplexität müssen neuen Prozesse entwickelt werden, zum Beispiel die Schulung von Personal gegen Social Engineering Angriffe, um die Sicherheit zu erhöhen. Und gerade in Public Clouds und auf geteilten Infrastrukturen wandelt sich der Aufbau von Schutzmechanismen. So müssen Systeme nicht mehr nur vor Angriffen von außerhalb geschützt werden, sondern auch vor Angriffe von innen heraus. Mit der Verteilung auf verschiedenen und unbekannten Systemen erhöht sich die Komplexität und die Anzahl potentiellen Angriffspunkte deutlich. Nur eine sichere Verschlüsselung, die durch den Kunden selbst und nicht durch den Cloud-Anbieter erfolgt, kann einen zuverlässigen Schutz seiner Daten gewährleisten. Ebenso sind starke Authentizität- und Zugangskontrollen notwendig um sicherzustellen, dass kein unbefugter Zugriff ausgeführt wird.

In Bereich der Transparenz haben Cloud-Anbieter noch starken Aufholbedarf und müssen neue Methoden entwickeln um rechtskonforme Dienste zu ermöglichen und damit auch das berechtigte Vertrauen der Kunden zu gewinnen. Neben der Anstrengungen der Anbieter müssen jedoch auch die Forschung, die Wirtschaft und Behörden gemeinsam neue Schutzstandards erarbeiten und entwickeln um eine gemeinsam rechtliche Basis zu schaffen.

Autoreninformation

Tobias Scheible arbeitet als wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen am Verbundprojekt Open Competence Center for Cyber Security. In dem Projekt werden nebenberufliche Fort- und Weiterbildungsmaßnahmen entwickelt, wie beispielsweise der Bachelor-Studiengang IT-Sicherheit und der Master-Studiengang IT-Compliance, E-Fraud & E-Discovery. Außerdem ist der Autor begeisterter Web-Entwickler und schreibt in seinem Blog unter http://scheible.it über seine Ideen, Erfahrungen und die Faszination des Internets.
Internet: http://scheible.it
Twitter: @TobiasScheible

Quellen

[1] http://scripting.com/disruption/mail.html
[2] http://winfwiki.wi-fom.de/index.php/Kostensenkungspotenzial_durch_Cloud_Computing
[3] http://www.bundestag.de/dokumente/analysen/2010/cloud_computing.pdf
[4] http://de.wikipedia.org/wiki/Geschichte_des_Internets#Dotcom-Boom_Ende_des_20._Jahrhunderts
[5] http://www.heise.de/netze/meldung/Telekom-schaltet-erste-Glasfaseranschluesse-1666557.html
[6] http://www.golem.de/news/google-fiber-ansturm-auf-1-gbit-s-fuer-70-us-dollar-1209-94469.html
[7] http://www.golem.de/1104/82945.html
[8] http://de.wikipedia.org/wiki/Cloud_Computing#Organisatorische_Arten_von_Clouds
[9] http://www.cloud-practice.de/know-how/ebenen-von-cloud-services
[10] http://www.prozeus.de/imperia/md/content/prozeus/broschueren/prozeus_broschuere_cloudcomputing_web.pdf
[11] http://www.stiftungaktuell.de/files/cloudcomputing_winkelmann.pdf
[12] http://www.zeit.de/2011/08/Cloud-Computing
[13] https://www.rsa.com/innovation/docs/10764_CLWD_BRF_1009_DE.pdf
[14] http://www.zdnet.de/41540830/hacker-knackt-passwoerter-mithilfe-der-amazon-cloud/
[15] http://www.computerwoche.de/management/it-strategie/2362186/
[16] http://www.it-business.de/news/recht/vorschriften-regulierungen/compliance/articles/253091/
[17] http://www.searchsecurity.de/themenbereiche/sicherheits-management/compliance/articles/292425/
[18] http://www.welt.de/wirtschaft/webwelt/article12680570/Beim-Cloud-Computing-drohen-gefaehrliche-Luecken.html
[19] http://www.wolke.hs-furtwangen.de/assets/files/Sicherheitsprobleme_fuer_IT-Outsourcing_durch_Cloud_Computing2.pdf