Luigi Lo Iacono

(E-Mail: l.lo_iacono@eufh.de)
studierte Technische Informatik an der Universität Siegen mit einem Schwerpunkt auf Kommunikations- und Informationssicherheit und promovierte 2005 im Bereich elektronischer Signaturen und PKI. Nach der Promotion arbeitete er in industriellen Forschungseinrichtung von Siemens in München und NEC Europe in Sankt Augustin und Heidelberg an eHome, Grid, SOA und Cloud Security Themen. Aktuell lehrt Luigi Lo Iacono im Fachbereich Wirtschaftsinformatik an der Europäischen Fachhochschule in Brühl.

Bevor der Sturm aus der Wolke bricht – ausgewählte Aspekte der Cloud-Security

Die Cloud ist längst kein Hype-Thema mehr. Auf Gartners Hype Cycle for Emerging Technologies des Jahres 2010 hat sie den Peak traversiert und ist auf dem besten Weg ins Tal der Ernüchterung [gar]. Übersteht sie diese Talsohle, so werden ihr noch zwei bis fünf Jahre eingeräumt, bis sie es zur breiten Massenanwendung geschafft haben könnte. Aktuelle Zahlen des Cloud-Pioneers unterstreichen diese Annahme mit Nachdruck [aws]. Waren im vierten Quartal 2009 noch 102 Milliarden Datenobjekte in der Amazon Speicherlösung S3 enthalten, stieg diese Zahl bis zum vierten Quartal 2010 um 256 % auf 262 Milliarden Datenobjekte an. Die maximale Anzahl an Anfragen, die an den S3-Dienst pro Sekunde gerichtet werden, wird mit 200.000 beziffert. Eine ganze Reihe anderer Indikatoren zeichnen ein ähnliches Bild. Höchste Zeit sich aktiv mit dem Thema auseinanderzusetzen. Was steckt denn nun hinter dieser Cloud?

Das kleine Cloud-Einmaleins

Obwohl der Begriff einer nicht-wissenschaftlichen Feder entsprang, haben sich mit der Zeit die zugrunde liegenden Konzepte und Technologien in eine wohldefinierte Struktur eingegliedert, die den Rahmen für eine methodische Herangehensweise an das Thema Cloud erlaubt. Einen wesentlichen Beitrag hierzu hat die US-Amerikanische Standardisierungsorganisation NIST geleistet [Mel09]. Der Quader in Abbildung 1 vereint diese Begriffe und stellt sie mit typischen Anwendungsdomänen dar.

Eine Unterscheidung kann gemäß der bereitgestellten Dienste getroffen werden. Wird Basisinfrastruktur in Form von z. B. Prozessoren, Hauptspeicher und Datenspeicher zur bedarfsgerechten Verwendung angeboten, dann spricht man von *Infrastructure as a Service* (IaaS). Laufzeitumgebungen bzw. Plattformen zur Ausführung von zumeist Webanwendungen werden mit dem Begriff *Platform as a Service* (PaaS) zusammengefasst. Vollständige Anwendungen, die sich vom Cloud-Anbieter im Bedarfsfall ohne Installation nutzen lassen, werden *Software as a Service* (SaaS) genannt.

Die Art und Weise, wie diese Dienstnutzungsmodelle verwendet werden, ermöglicht eine weitere Klassifizierung. Werden die eigenen Ressourcen mithilfe von Cloud-Konzepten und -Technologien flexibler und effizienter nutzbar gemacht, so spricht man von einer *Private Cloud*, da diese ausschließlich dem Betreiber zur

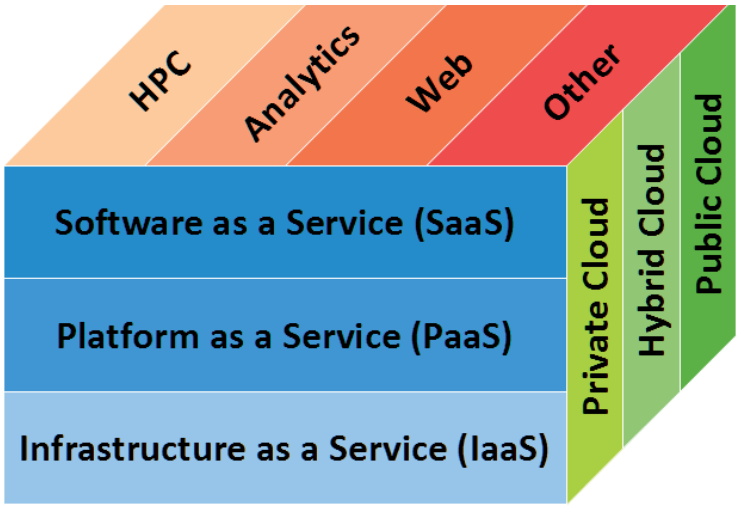

Abb. 1: Cloud-Begrifflichkeiten auf einen Blick [Mat09]

Verfügung steht. *Public Clouds* stellen hingegen Angebote dar, die für jeden nutzbar sind. Ein Anbieter von Public Cloud-Diensten stellt seine Ressourcen allen Kunden zur Verfügung, die diese gemeinsam nutzen. Die Kombination aus diesen beiden Ansätzen wird *Hybrid Cloud* genannt. Hierbei wird auf Public Cloud-Dienste zurückgegriffen, sobald die eigene Private Cloud für die aktuelle Arbeitslast nicht ausreichend ist.

Aus den Diskussionen zu den Dienstbetriebsmodellen wird ersichtlich, dass sich

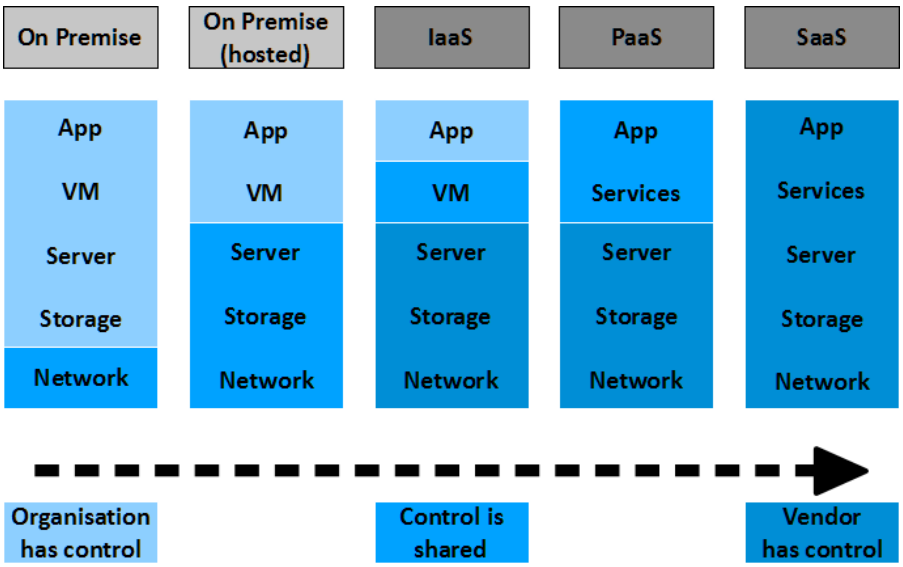

Abb. 2: Governance-Struktur in der Cloud [Mat09]

Cloud-Anbieter in zwei Gruppen unterteilen: Anbieter von Public Cloud-Diensten und Anbieter von Produkten und Lösungen zur Umsetzung von Private Clouds.

Das Versprechen der Cloud liegt in Kostenersparnissen bei der Anschaffung (Investitionsaufwand), dem Betrieb und der Wartung (Betriebsaufwand) des eigenen Rechnerparks. Als größter „Hemmschuh" wird die Informationssicherheit in der Cloud gesehen [blo]. Dies gilt insbesondere für Architekturen, die auf den Dienstbetriebsmodus Public Cloud setzen.

Die Cloud durch die Sicherheitsbrille betrachtet

Was bedeutet es, aus Sicherheitssicht sich (Public) Cloud-Diensten zu bedienen? In erster Linie einmal Kontrollverlust. Abbildung 2 zeigt schematisch, wie sich dies zu den Cloud-Dienstemodellen verhält. Zur besseren Verdeutlichung werden diese den herkömmlichen Verwendungsszenarien gegenübergestellt. Das Betreiben eigener Ressourcen in eigenen Räumlichkeiten (On-Premise) bedeutet die höchste Kontrolle, da bis auf den Anschluss an das WAN alles in den eigenen Händen liegt. Bei der Nutzung von Hosting-Angeboten geht zusätzlich zum Netzzugang die Kontrolle der Server und der Speicherkapazitäten an den entsprechenden Anbieter über. Bei IaaS-Angeboten kommt die Virtualisierungsschicht hinzu, wobei einige Kontrollfunktionen beim Anbieter verbleiben. Bei PaaS-Angeboten gilt das für die Plattform-Dienste und die Anwendung. Die Kontrolle beim SaaS-Modell geht vollständig auf den Anbieter über.

Hohe Kontrolle bedeutet in der Regel einen höheren Aufwand und damit einhergehend höhere Kosten beim Betrieb der IT-Ressourcen. Auf der anderen Seite können Fragen wie:

- Wo befinden sich meine Daten, Programme, Prozesse?
- Wer hat Zugriff darauf?
- Wie belastbar und zuverlässig sind die Dienste?
- Wie und wie oft werden die Dienste von unabhängigen Stellen geprüft?
- Wie kann das eigenen Sicherheitspersonal den Sicherheitszustand prüfen?

klar und bestimmt beantwortet werden. Es gilt also, die richtige Balance zwischen den möglichen Kostenersparnissen und dem Kontrollverlust in Abhängigkeit zum konkreten Anwendungsfall zu finden. Hierzu muss das Verständnis für die Gefahren vorhanden sein, um entsprechende Risiken für den konkreten Anwendungskontext bestimmen und einschätzen zu können.

Gefahrenortungsplan

Wo kann denn überhaupt etwas passieren und was genau kann passieren? Auf diese Fragen kann mit Abbildung 3 eine strukturierte Antwort gegeben werden.

Geht man das in Abbildung 3 dargestellte Schichtenmodell von oben nach unten durch, sind zunächst Gefahrenpotenziale im Client, womit auf die Cloud-Dienste zugegriffen wird, zu berücksichtigen. Der Client kann unterschiedlich ausgeprägt sein und von kommandozeilenbasierten Tools über GUI-basierte Programme bis hin zu Webanwendungen reichen.

Generell muss darauf geachtet werden, dass die Client-Systeme frei von Schadsoftware sind. Zudem sollten auf diesen Systemen keine Zugangsdaten zur Cloud

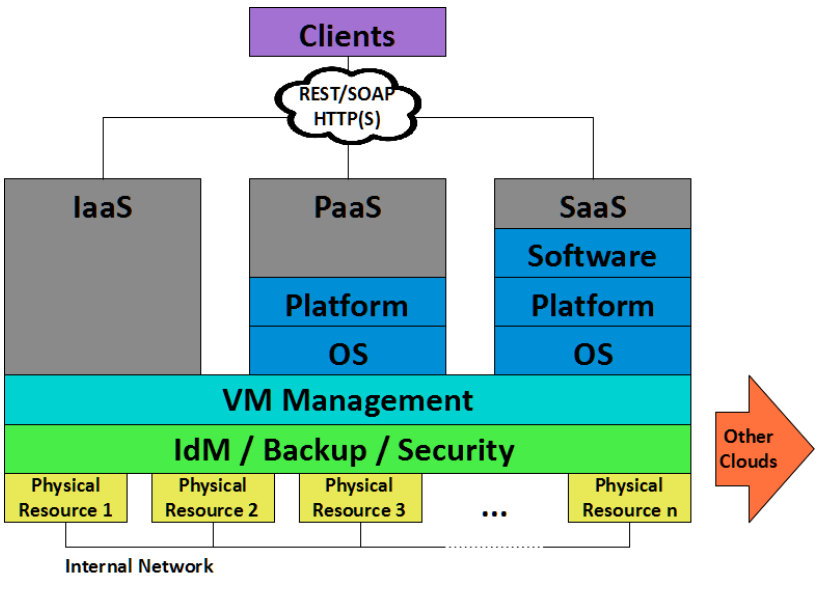

Abb. 3: Schichtenmodell der Cloud [Frö10]

hinterlegt sein, da diese das Ziel von „Angreifern“ sind, um sich auf Kosten anderer, IT-Ressourcen für ihre eigenen Zwecke zu erschleichen. Da häufig ein Webbrowser als Client verwendet wird, muss in diesen Fällen insbesondere die erhöhte Anfälligkeit dieser gegen Angriffe über die zahlreichen Browsererweiterungen bzw. spezifische Angriffe auf Webanwendungen, wie z. B. SQL Injection, Cross-site Scripting und Cross-site Request Forgery, berücksichtigt werden.

Die nächste zu betrachtende Komponente ist der Kommunikationskanal zwischen dem Client und den Cloud-Diensten. Technisch wird der Kommunikationszugang zu den Cloud-Diensten zumeist mit dem REST-Konzept oder dem Protokoll SOAP realisiert. In beiden Fällen kommt HTTP als Transportvehikel zum Tragen. Die Kommunikation zu REST-basierten Dienstschnittstellen lässt sich mittels SSL/TLS schützen. Dieses Protokoll etabliert einen vertraulichen, integeren und authentifizierten Kanal zwischen Webbrowser und Webserver.

Hierbei gilt es unbedingt zu beachten, dass die SSL/TLS-gesicherte Kommunikation beim Webserverprozess endet und die Daten damit, in Szenarien einer entfernten oder verteilten Anwendungslogik, für weitere Kommunikationsstrecken erneut zu sichern sind. Für SOAP stehen weitreichendere Sicherheitsmechanismen bereit, die auf Grundlage von WS-Security [oas] in die SOAP-Nachrichten integriert werden und damit von Ende-zu-Ende reichen.

Dennoch gilt es auch hier, sehr umsichtig mit der Implementierung dieser Sicherheitsmechanismen zu sein, damit diese nicht ausgehebelt werden können, wie es z. B. mit sogenannten XML Signature Wrapping-Angriffen auf signierte SOAP-Nachrichten erfolgen kann [nds]. Hier ist insbesondere der Cloud-Anbieter in der Pflicht, entsprechende Sorgfalt walten zu lassen und Prozesse vorzusehen, die die Effektivität der eigenen Schutzmechanismen fortlaufend überwachen und überprüfen.

Über den Kommunikationskanal können die Cloud-Dienste zudem von Denial-of-Service (DoS) Angriffen heimgesucht werden. DoS-Angriffe bekommen durch die Cloud eine neue Dimension. Hatten sie zuvor das Ziel, einen Dienst (meist durch eine überfordernde Anzahl an Anfragen) lahm zu legen, ist dies in der Cloud durch die sich dynamisch anpassenden Ressourcen nicht ohne weiteres möglich. Es stellt sich jedoch der Effekt ein, dass durch eine Anfrageflut die Kosten auf der Seite des angegriffenen Cloud-Kunden ansteigen. Diese Inkarnation des Angriffs wird deshalb auch als Economic Denial of Sustainability (EDoS) bezeichnet [rat].

Anschließend muss zwischen den Dienstnutzungsmodellen unterschieden werden. IaaS bietet sehr elementare und universell einsetzbare Dienste. So können z. B. neben den für die Ausführung in der Cloud bestimmten Programmen und Daten zusätzliche Komponenten installiert werden, die für eine erhöhte Sicherheit sorgen. Hierunter zählen u. a. Firewalls, IDS und SIEM-Systeme.

Ein derartiger Freiheitsgrad ist bei PaaS und SaaS nicht gegeben. Hier kann der Anwender nur auf das zurückgreifen, was der Anbieter bereitstellt. Gerade im PaaS-Umfeld ist Nachholbedarf zu erkennen. Um Webanwendungen gegen Angriffe wie SQL Injection, Cross-site Scripting oder Cross-site Request Forgery zu schützen, kann z. B. eine Web Application Firewall (WAF) eingesetzt werden. Die Integration eines derartigen Sicherheitsmoduls im zugrunde liegenden Webserver würde dem Anwender einiges an Arbeit ersparen, die auf das Festlegen von Filterregeln beschränkt wäre. Die meisten PaaS-Anbieter stellen diesen Zusatzdienst bisher nicht zur Verfügung und lassen den Anwender damit auf sich selbst gestellt. Der Anwender muss daher häufig WAF-Funktionalitäten in seiner Anwendung verankern und bei der Inbetriebnahme der Anwendung mit auf die Plattform bringen.

Bei der Verwendung von kompletten Anwendungen nach dem SaaS-Modell ist die Abhängigkeit vom Anbieter noch größer und die Möglichkeit eigene Vorkehrungen zu treffen faktisch ausgeschlossen. Im Dialog mit dem Anbieter sollten allerdings Absprachen getroffen werden, die den Anwender in die Lage versetzen, sich einen Überblick über den Sicherheitszustand und die Nutzung zu verschaffen. Das kann von entsprechenden Frontends, die Monitoringdaten aufbereiten und visualisieren, bis hin zur Erlaubnis die SaaS-Anwendung des Anbieters zu penetrieren, gehen.

Eine weitere anfällige Komponente kann die Virtualisierungsschicht sein. Schwachstellen im Hypervisor könnten ausgenutzt werden und dazu führen, dass Unbefugte sich Zugriff auf das Hostsystem verschaffen. Von dort können sie dann auf die weiteren Gäste des Hosts zugreifen. Dass es möglich ist, eine eigene virtuelle Maschine auf den gleichen Host einer bestimmten, evtl. vom Angreifer gesuchten, virtuellen Maschine zu positionieren, zeigt die Arbeit von Thomas Ristenpart und seinen Mitautoren [cse]. Dadurch erhalten Hypervisor-basierte Angriffe eine neue Brisanz, der man nur mit konsequenten und zeitnahen Updates begegnen kann.

Die verbleibenden Schichten sind nicht Cloud-spezifisch und können nach bewährten Methoden umgesetzt werden. Beispiele hierfür sind, dass Backups verschlüsselt abgelegt werden müssen und dass administrative Arbeiten an den Systemen, die sensitive Kundendaten vorhalten, nur nach dem Vier-Augen-Prinzip durchgeführt werden dürfen. Der Anwender sollte bei der Auswahl eines Anbieters über derartige Praktiken informieren.

Zurück zu zentralisierten Strukturen

Allgemein kann festgehalten werden, dass die Cloud, unter der Annahme, dass sich diese in einer marktbereinigten und konsolidierten Ausprägung in den Händen einiger weniger Anbieter befindet, eine zentralisierte Infrastruktur bildet, die kaum mehr den ursprünglichen Zielen des Internets gerecht werden kann. So zeichnet sich bereits heute ab, dass sich Ausfälle durch Fehler oder Katastrophen nicht durch das dynamische Umleiten des Datenverkehrs umschiffen lassen.

Ein aktuelles Beispiel vom 21. April 2011 zeigt, wie ein fehlerhafter Backup-

Prozess Amazons EC2 Web-Hosting Dienst in der Region US-EAST-1 für sieben Stunden außer Gefecht gesetzt und damit eine Lawine ins Rollen gebracht hat, die bekannte Websites wie Foursquare, Quora, Hootsuite und Reddit mit sich gerissen hat [new]. Clouds müssen an dieser Stelle deutlich offener werden, damit in solchen Fällen ein automatisches Umschalten auf andere Clouds erfolgen kann.

Aus Fehlern lernen

Neben der Sogwirkung wird an diesem Vorfall zudem ersichtlich, wie wichtig eine transparente Informationspolitik des Anbieters ist. Im Forum finden sich viele kritische Stimmen, die genau diese zeitnahen Informationen vermissen. Die Inbetriebnahme einer Notlösung wird dadurch nur unnötig erschwert. Auf der anderen Seite zeigt das, wie wichtig es ist, auf derartige Ausfälle vorbereitet zu sein.

Die privat betriebene, nicht-gewinnorientierte Open Security Foundation betreibt eine Web-Plattform als unparteiische Sammelstelle für Vorfälle rund um Cloud-Security. Unter dem Namen *Cloutage* (zusammengesetzt aus Cloud und Outage) wird eine Datenbank aufgebaut, die aus Medienberichten und anonymen Hinweise aus der Community gespeist wird [clo].

Viel besorgniserregender ist aber eine weiterere Meldung, die von einem Unternehmen in das Forum eingetragen wurde, das (hunderte!) herzkranker Menschen beobachtet und dies auf Grundlage der Amazon Cloud tut. Im Forumseintrag lässt sich lesen, dass die EKG-Werte, der unter Beobachtung stehenden Menschen, (seit dem Ausfall) nicht mehr abgerufen werden konnten [for]. Offenkundig ist hier nicht die richtige Balance zwischen Kostenreduzierung und Kontrollverlust gefunden worden, die in diesem Artikel als Notwendigkeit hervorgehoben wurde.

Fazit

Trotz der bestehenden Sicherheitsherausforderungen kommt man vermutlich nur schwer an der Cloud vorbei. In Abhängigkeit der Domäne und des konkreten Kontextes ist die Verwendung von Cloud-Diensten mehr oder weniger gradlinig umsetzbar. Die gegebenen Sicherheitsanforderungen sowie die involvierten Daten und deren Sensitivität spielen hierbei eine entscheidende Rolle. Aktuelle Beispiele zeigen immer wieder, dass hiermit noch zu leger verfahren wird.

Da die Forschergemeinde rege an innovativen Ansätzen arbeitet und diese Schritt-für-Schritt von den Anbietern in ihre Dienste aufgenommen werden, bleibt das Thema im Fluss, was Security ohnehin – als Prozess aufgefasst – immer sein sollte. ■

Literatur & Links

[gar] http://www.gartner.com/it/page.jsp?id=1447613

[aws] http://aws.typepad.com/aws/2011/01/amazon-s3-bigger-and-busier-than-ever.html

[Mel09] P. Mell, T. Grance: The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Version 15, 2009

[blo] http://blogs.idc.com/ie/?p=210

[Mat09] T. Mather, S. Kumaraswamy, S. Latif: Cloud-Security and Privacy, O'Reilly, 2009

[Frö10] H.-P. Fröschle, S. Reinheimer (Herausgeber): Cloud Computing & SaaS, Dpunkt, 2010

[oas] http://www.oasis-open.org/committees/wss/

[nds] http://www.nds.rub.de/media/nds/downloads/mjensen/ICWS09.pdf

[rat] http://rationalsecurity.typepad.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-service-to-edos-economic-denial-of-sustaina.html

[cse] http://cseweb.ucsd.edu/~hovav/papers/rtss09.html

[new] http://www.newscientist.com/blogs/onepercent/2011/04/amazon-server-failure-knocks-o.html

[clo] http://cloutage.org

[for] https://forums.aws.amazon.com/thread.jspa?threadID=65649&tstart=0