

TClouds

Herausforderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud

Das von der Europäischen Kommission geförderte Projekt TClouds hat die Entwicklung einer sicheren und datenschutzkonformen Cloud-Infrastruktur zum Ziel. Dieser Beitrag beschreibt die Herausforderungen und die ersten Lösungsideen.

Einführung

Cloud Dienste versprechen die bedarfsgerechte Bereitstellung von IT-Leistungen über standardisierte Schnittstellen im Internet. Die Abrechnung erfolgt per Nutzung und die Ressourcen skalieren mit dem Bedarf der Anwender. Aus fixen Investitionen für eine hausinterne IT werden variable Kosten, aus einer starren hausinternen IT Infrastruktur wird ein flexible und dynamische Dienstleistung. Auch wenn diese Charakteristika perfekt in die heutigen schnelllebigem und flexiblen Geschäftsprozesse passen, gibt es eine Reihe von Problemen, die einer breiten Akzeptanz von Cloud Computing im Unternehmensumfeld im Wege stehen. Insbesondere muss hier zunächst das Vertrauen der Anwender in eine gleichermaßen sichere als auch rechtskonforme Verarbeitung sensibler Anwenderdaten durch die Cloud Anbieter geschaffen werden. Gemäß der Studie "Security and the Cloud" (Penn, 2010) des Marktforschungsunternehmens Forrester Research wird der Markt für Cloud Sicherheitslösungen bis 2015 auf USD 1.5 Milliarden anwachsen.

Über TClouds

Das von der Europäischen Kommission geförderte Projekt „TClouds - Privacy and Resilience for Internet-scale Critical Infrastructure“ mit einer Laufzeit vom 01.10.2010 bis 31.09.2013 hat das Ziel eine vertrauenswürdige und hochzuverlässige Cloud-Infrastruktur zu entwickeln. Diese ermöglicht dem Anwender eine nachvollziehbare und revisionssichere Verarbeitung personenbezogener oder anderer sensibler Daten, ohne den Aufbau einer physisch getrennten privaten Cloud zu erfordern. Primär betrachtet TClouds die

Infrastruktur-Cloud, auf der Dienste wie Platform-as-a-Service oder Software-as-a-Service aufbauen können.

Das Konsortium aus 14 Partnern bestehend aus Universitäten, Unternehmen, Behörden und Anwendern bearbeitet ein breites Spektrum von Aufgaben und Herausforderungen im Cloud Computing:

- Entwicklung von vertrauenswürdigen Clouds, die föderativ in einer Architektur zusammenwirken. Dies umfasst sowohl den Entwurf neuer Basistechnologie, als auch die Einbindung von heute schon kommerziell verfügbaren Cloud Angeboten.
- Beschreibung der rechtlichen und sozioökonomische Anforderungen an grenzüberschreitende Clouds sowie die Evaluation der technischen Projektergebnisse.
- Demonstration und Validierung der technischen Projektentwicklungen an zwei Prototypen aus dem Gesundheitsbereich und dem Energiesektor.
- Unterstützung von Standardisierungsbestrebungen durch die Zusammenarbeit mit anderen Cloud-Initiativen.

Sicherheitsprobleme des Cloud Computing

Als neuartige Technologie birgt Cloud-Computing auch entsprechend neue Sicherheitsrisiken (Cloud Security Alliance, 2010). Im folgenden beschreiben wir zentrale Risiken des Cloud Computing (Glott et. al., 2011). Folglich sind eine sorgfältige Kontrolle und Bewältigung von Sicherheitsrisiken unabdingbar (Kaliski & Pauley, 2010).

Heutige Rechenzentren: Maßstab für die Cloud

Einsatz von Technologie für kritische Anwendungen ist in der Regel risikobehaftet. Sollte eine verwendete Cloud Infrastruktur ausfallen, hätte das gravierende Auswirkungen. Selbst wenn mehrstufige Sicherheitslösungen vorhanden sind (z.B. Firewall, Schutzmechanismen gegen unerlaubten Zugriff und Schutz jedes einzelnen Servers), enthalten nahezu alle Systeme Fehler, die gefunden und ausgenutzt werden können. Offline-Systeme sind zwar schwieriger anzugreifen, aber der Austausch von Speichermedien, wie z.B. USB-Speicher, ermöglicht es, auch Systeme anzugreifen, die nicht mit dem Internet verbunden sind (Chien, 2010).

Cloud-Sourcing liegt mehr oder weniger das gleiche wirtschaftliche Prinzip wie dem traditionellen Outsourcing von IT zu Grunde. Es bietet aber mehr Vorteile, u.a. bezüglich Upgrades und Patches, schnellerer Beschaffungsdienstleistungen, der Vermeidung von Herstellerabhängigkeit und der Systemmodernisierung (Rajan, 2010). Aus unserer Sicht, sollten die heutigen Rechenzentren als Maßstab für die Sicherheitsvorgaben bei der Verwendung von Clouds herangezogen werden. Insgesamt müssen die Vorteile die möglichen Nachteile und Risiken überwiegen. Die Quantifizierung der Vorteile bezüglich Kosten und Flexibilität ist wesentlich einfacher, als eine qualitative und quantitative Erfassung möglicher Nachteile oder Risiken. Wichtig ist hier, Sicherheitsrisiken abzuschätzen, um den Unternehmen die Auswahl jener Anwendungen zu ermöglichen, welche mit dem angebotenen Sicherheitsniveau auskommen. Heute macht es das

unbekannte Restrisiko unmöglich solche Risiko-Managemententscheidungen zu treffen. Hierdurch werden derzeit meist nur unkritische Anwendungen auf Clouds ausgelagert.

Bezüglich der Sicherheit lassen sich aus diesem Argument heraus zwei Forderungen für den Einsatz von Clouds in Unternehmen ableiten. Erstens, bezüglich Sicherheit und Vertrauen werden neue Lösungen, wie die Cloud oder die sog. Cloud-of-Clouds, mit bestehenden Lösungen, wie unternehmenseigene oder externe Rechenzentren, verglichen und beurteilt. Zweitens müssen Unternehmen die Cloud-Infrastruktur in ihr Gesamtrisikomanagement integrieren können, um eine Migration auch kritischer Anwendungen in die Cloud zu ermöglichen.

Fehlende Trennung zwischen Kunden

Cloud-Umgebungen realisieren Skalierbarkeit durch die gemeinsame Verwendung von Ressourcen durch mehrere Kunden. Dadurch erhöht sich das Risiko von Geheimhaltungsverletzung und Dienst-Unterbrechungen, welche sich durch solche gemeinsam genutzten Ressourcen fortpflanzen können. Von zentraler Bedeutung ist hierbei, dass kein unerlaubter Informationsfluss zwischen Kunden erfolgt und dass eine Fehlfunktion oder ein Fehlverhalten bei einem Kunden nicht zu Verletzungen der Leistungsverträge von anderen Kunden führen kann.

Das traditionelle Outsourcing in Unternehmen gewährleistet die mandantenfähige Kundentrennung (die sog. "multi-tenant isolation") durch die feste Zuordnung von Ressourcen an den einzelnen Kunden und durch die Löschung aller Ressourcen vor der Wiederverwendung durch andere Kunden. Das Teilen von Ressourcen und Mandanten-Isolation können auf verschiedenen Abstraktionsebenen implementiert werden:

- "Grobkörnigere" Mechanismen wie gemeinsame Datenzentren, Hauptrechner und Netze sind gut erforscht und die gewünschte Isolation kann durch Technologien wie Virtuelle Rechner, vLAN oder SAN erzielt werden.
- Das Teilen von Ressourcen, wie Betriebssysteme, Middleware oder sogar Software, erfordert fallspezifische und maßgeschneiderte Isolationsmechanismen. Speziell das

letztenannte Beispiel, die Software als Dienstleistung (die sog. Software-as-a-Service) erfordert, dass jede Dateninstanz einem Kunden zugeordnet ist und dass kein anderer Kunde auf diese Dateninstanzen Zugriff nehmen kann.

In der Praxis kommen allerdings oft Mischformen dieser Mechanismen vor. So kann ein Kunde z.B., eine eigene virtuelle Maschine besitzen (Isolation auf Maschinenebene), diese Maschine aber wiederum einen gemeinsam verwendeten Datenbankserver benutzen (Isolation durch Middleware).

Um dieses Risiko in einer Cloud-Computing Umgebung zu entschärfen, gewährleistet die mandantenfähige Isolation die Isolation der Kunden. Ein Prinzip solche Isolation zu implementieren ist durch Kennzeichnung und Flusskontrolle.

■ **Kennzeichnung:** Alle Ressourcen sind einem Kunden zugeordnet und mit einer entsprechenden Kennzeichnung versehen.

■ **Flusskontrolle:** Gemeinsam benutzte Ressourcen müssen den möglichen Datenfluss überwachen und gewährleisten, dass zwischen den einzelnen Kunden kein unautorisierte Datenfluss stattfindet. Um die Flusskontrolle zu beschränken können auch Mechanismen wie Zugriffskontrolle sicherstellen, dass die Maschinen und Applikationen eines Kunden weder auf Daten noch auf die Ressourcen eines anderen Kunden Zugriff nehmen können.

In der Praxis ist die Identifizierung und Verhinderung von allen unerwünschten Informationsflüssen eine wichtige Herausforderung (Ristenpart et. al., 2009), da alle gemeinsam genutzten Systeme diese Prinzipien durchsetzen müssen (Cabuk et. al., 2010).

Insider-Angriffe durch die Cloud-Betreiber

Ein weiteres bedeutendes Sicherheitsrisiko ist das unbeabsichtigte oder böswillige Fehlverhalten von Insidern. Beispiele hierfür sind ein Netzwerkadministrator, der Datenbankoperationen beeinflusst, oder Administratoren die Daten stehlen und weitergeben. Die Eindämmung dieses Risikos ist schwierig, da die Sicherheitskontrollen den Verwaltungsaufwand nicht wesentlich erhöhen dürfen und insbesondere Fehlerbehebung weiterhin effizient möglich sein muss.

Ein klassischer Ansatz, dieses Risiko einzuschränken, ist die konsequente Umsetzung von Rechteminimierung (das „least privilege principle“) im Cloud-Management System. Dies bedeutet unter Anderem, dass dem Cloud-Management System eine feinmaschige Hierarchie von Rollen mit genauer Aufgabentrennung zu Grunde liegt. Das Ziel hierbei ist, dass jeder Administrator nur gerade jenes Minimum an Privilegien hat, das notwendig ist, um die jeweilige Aufgabe zu erfüllen. Während heute ein Computer-Operator fast schon Allmacht hat, können mit der Einführung des Prinzips der kleinstmöglichen Privilegien folgende Ziele erreicht werden:

- Infrastruktur-Administratoren können ihre Infrastruktur modifizieren (Netzwerk, Speichermedien, Maschinen), haben aber keinen Zugriff auf gespeicherte oder transportierte Daten.
- Sicherheitsadministratoren können Verfahren definieren, aber sonst keine weitere Rolle mehr belegen.
- Mitarbeitende eines Kunden können Zugriff auf ihre jeweiligen Daten und Systeme (oder auf Teile davon) nehmen, aber nicht auf die Infrastruktur oder Daten anderer Kunden.
- Alle Administrationszugriffe werden aufgezeichnet und können im Nachhinein validiert werden.

Diese Verwaltung privilegierter Identitäten kommt zunehmend in traditionellen Rechenzentren zum Einsatz und sollte für sichere Cloud-Lösungen Standard sein. In den heutigen Datenzentren, in denen Managementaufgaben oft ins Ausland verlagert werden, wird so sichergestellt, dass ein negativer Einfluss von Administratoren in Übersee eingeschränkt werden kann. Langfristig können praktische Vorgehensweisen, wie das privilegierte Identitätsmanagement mit stärkeren Schutzmechanismen, wie z.B. das sog. Trusted Computing (Santos et. al., 2009) oder Berechnungen auf ausgelagerten Daten (Sadeghi et. al., 2010) ergänzt werden.

Schwachstellen in Cloud-Management Systemen

Aufgrund des hohen Automatisierungsgrades von Cloud-Management Systemen und der hohen

Komplexität der verwalteten Systeme, kommt der Qualität der Cloud-Software eine zentrale Bedeutung bei der Vermeidung von Dienstunterbrechungen und Ausfällen zu. Cloud-Systeme erhöhen die Effizienz durch „Industrialisierung“ der Bereitstellung von IT-Dienstleistungen mittels umfassender Automatisierung. Das bedeutet, dass wenn ein Fehler in solch komplexen und automatisierten Systemen auftritt, eine manuelle Intervention, um Fehler zu entdecken und zu beheben, zu weiteren Fehlern führen kann. Ebenso ist es wahrscheinlich, dass sich Fehler aufgrund der globalen Ausdehnung solcher Systemweltweit reproduzieren und somit auch deren Behebung automatisiert werden muss. Eine weitere Störungsquelle entsteht dadurch, dass groß angelegte Computing-Clouds oft aus preisgünstiger Standardhardware aufgebaut werden, die (relativ) störungsanfällig ist. Dies führt zu häufigen Ausfällen von Maschinen, die auch einen Teilbereich der Management-Infrastruktur umfassen können. Die Konsequenz ist, dass in einer Cloud-Umgebung gemeinhin automatisierte Fehlertoleranz-, Fehlerfindungs- und (Selbst-)Reparaturmechanismen zur Wiederherstellung nach Soft- oder Hardwarefehlern benötigt werden. Wichtige Werkzeuge für die Erstellung solcher widerstandsfähiger Systeme sind Datenreplikation, atomare Aktualisierungen von replizierten Managementdaten und Integritätschecks aller erhaltenen Daten (z.B. Vukolic (2010)). Längerfristig kann die in TClouds praktizierte Verwendung mehrerer Clouds die Widerstandsfähigkeit noch weiter erhöhen.

Mangel an Transparenz und Garantien

Die oben vorgeschlagenen Mechanismen zur Begrenzung der aufgezeigten Risiken sind zwar wichtig, doch bleiben Sicherheitszwischenfälle oft unerkannt. So können z.B. Datenverfälschungen lange unentdeckt bleiben. Eine Datenweitergabe durch einen geschickten Insider wird selten aufgedeckt. Außerdem werden in der Regel weder der operationelle Zustand noch mögliche Probleme dem Kunden mitgeteilt.

In einer Cloud-Umgebung ist heute ein „Black-Box“-Ansatz üblich, bei dem der Kunde weder Einsicht in die Cloud-Infrastruktur nehmen kann noch einen

Beweis für deren fehlerfreien Betrieb erhält. Wir sehen die Abkehr von diesem Ansatz für kritische Anwendungen als zwingend an. Ähnlich gelagert ist auch die Herausforderung, wie das Vertrauen der Kunden in einen korrekten Betrieb der Cloud-Infrastruktur am besten gefördert wird. Nachstehend werden einige Teillösungen umrissen, doch existiert noch keine allgemein akzeptierte Musterlösung im Sinne einer „Best Practice“.

Am häufigsten ist der so genannte „nach bestem Wissen und Gewissen“-Ansatz (engl. „best effort“), bei dem die Betreiber versprechen, „ihr Möglichstes zu tun“ aber keine konkreten Garantien geben. Dieser Ansatz ist heute bei gratis Cloud-Angeboten die Regel. Eine Verbesserung davon stellt die Prüfung durch neutrale Sachverständige dar, wie sie heute beim Outsourcing die Regel ist. Hier werden (Cloud)-Dienstleistungszentren durch eine unabhängige Organisation auf die Einhaltungen wohldefinierter Standards wie ISO27001 oder SAS70 geprüft. So erhalten Kunden die Gewissheit, dass die Organisation zum Zeitpunkt der Zertifizierung diesen Standards entsprach. Dieser Ansatz ist zwar heute allgemein verbreitet, bedeutet aber trotzdem nur, dass die Bedingungen zu einem bestimmten Zeitpunkt erfüllt wurden, und kann, weil es ein Prüfung aufgrund von Stichproben ist, trotzdem Bereiche, die die Auflagen nicht erfüllen, übersehen, weil diese zufälligerweise nicht Teil der Prüfung waren. Mittelfristig erwarten wir, dass Cloud-Anbieter automatisierte Schnittstellen zur Überwachung und zur Störungsbehebung implementieren (Grobauer & Schreck, 2010). Damit werden Kunden automatisch von Vorfällen in Kenntnis gesetzt und können diese automatisiert analysieren und entsprechend reagieren.

Langfristig würden ideale Transparenzmechanismen die Implementierung von Prozessen in der Weise garantieren, dass die vereinbarten Prozeduren eingehalten werden, funktionelle wie auch nicht-funktionelle Auflagen erfüllt werden und keine Daten verfälscht oder Dritten zugespielt werden. In der Praxis sind diese Probleme weitgehend ungelöst. Eine geeignetere Methode ist die Verwendung des sog. Trusted Computing, um den korrekten Vollzug der Richtlinien zu verifizieren (Chow et. al., 2009). Die

Instantiierung von Trusted Computing, wie sie die Trusted Computing Gruppe (TCG) vorschlägt, verwendet sichere Hardware, damit ein Akteur eine Konformitätsbescheinigung durchführen kann, bzw. um einen Nachweis über die ausführbaren Dateien und die Konfiguration, die zum Boot-Zeitpunkt geladen wurden, zu erhalten. Eine entsprechende Lösung für einen vergleichbaren Nachweis zur Laufzeit ist und bleibt eine Herausforderung.

Und die Datenschutzrisiken?

Eine Grundvoraussetzung für vertrauenswürdigen Cloud-Computing ist Datenschutz (Weichert, 2009). Einfach gesagt, ist das Ziel von Datenschutz der Schutz von Daten, die einer Person zugeordnet werden können, der sog. personally identifying information (PII). In Europa ist das Recht auf Achtung von Privat- und Familienleben, Wohnung und Korrespondenz in Artikel 8 der Europäischen Menschenrechtskonvention (ECHR) festgelegt. Der Europäische Gerichtshof für Menschenrechte hat in vielen Entscheidungen festgelegt, dass dieser Artikel auch auf den Schutz der PII einer Person anwendbar ist. Des Weiteren werden diese Rechte durch die Datenschutzrichtlinie der EU-Kommission (95/46/EC) bekräftigt und konkretisiert, um ein umfassendes Datenschutzsystem in ganz Europa einzurichten. Diese Richtlinie trägt auch den OECD Datenschutzgrundsätzen Rechnung (Organization for Economic Co-Operation and Development, 2009), welche mehrere Prinzipien anordnet, wie z.B. die eingeschränkte Sammlung von Daten, das Vorliegen einer rechtlichen Grundlage oder einer aktiven Zustimmung der betroffenen Person (dem sog. „Data Subject“) für das Sammeln von Daten, das Recht auf Korrektur und Löschung der Daten sowie die Notwendigkeit von angemessenen Sicherheitsvorkehrungen zum Schutz der gesammelten Daten.

Da Cloud-Computing oft das Auslagern der Datenverarbeitung beinhaltet, besteht sowohl für den Benutzer wie auch für die betroffene Person die Gefahr eines Datenverlusts, einer Datenverfälschung oder des Abhörens während des Datentransfers an einen externen Cloud-Anbieter. Verwandt mit diesen de-facto Hemmnissen in Bezug auf die rechtlichen Voraussetzungen sind drei

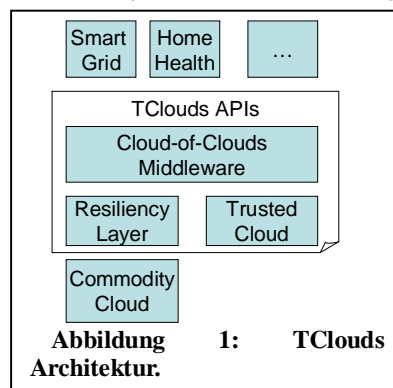
Probleme, die in allen Cloud-Lösungen angegangen werden müssen: Transparenz, technische und organisatorische Sicherheitsvorkehrungen und vertragliche Verpflichtung.

Gemäß der Europäischen Gesetzgebung ist derjenige Benutzer, der die PII in einer Cloud oder anderswo verarbeitet, verantwortlich für die Einhaltung der oben genannten Daten- und Datenschutzrichtlinien. Ein Outsourcing der Datenverarbeitung entbindet den Benutzer nicht von seiner Verpflichtung und Haftung bezüglich der Daten. Dies bedeutet, dass der Benutzer kontrollieren und verstehen kann, was mit den Daten in der Cloud passiert und welche Sicherheitsmechanismen implementiert sind. Damit der Benutzer diese rechtliche Verpflichtung wahrnehmen kann, muss die grösstmögliche Transparenz bezüglich der Prozesse innerhalb der Cloud bestehen. Technisch könnte dies z.B. umgesetzt werden, indem informative Logs über die Vorgänge und Zugriffe installiert werden, die es einem Benutzer erlauben, genau und detailliert nachzuvollziehen, was mit seinen Daten geschieht, wo sie abgespeichert werden und wer auf sie zugreift. Zudem könnte der Cloud-Dienstleister beweisen, dass angemessene Sicherheitsmaßnahmen bestehen, in dem er sich regelmäßig einer Überprüfung und Zertifizierung durch eine anerkannte Institution unterzieht. Rechtlich könnte die Einhaltung der europäischen Gesetzgebung im Rahmen einer Verpflichtung zur Einhaltung der verbindlichen unternehmensinternen Vorschriften (auf Englisch Bindung Corporate Rules oder kurz BCR) abgesichert werden. Eine weitere Möglichkeit ist die Einbindung von Leistungsvereinbarungen (englisch Service Level Agreements oder SLAs) in die Verträge, in denen die Einhaltung der spezifizierten Datenschutzerfordernungen zugesichert wird. Diese SLAs könnten z.B. die Einhaltung des Datenschutzes durch die Festsetzung von Vertragsstrafen in Falle einer Missachtung gewährleisten.

Dies ist speziell wichtig im Falle von länderübergreifenden Cloud-Computing mit Vertragsbeziehungen zu mehreren Cloud-Dienstleistern als Subunternehmer. Subunternehmer sind bereits die Regel im Bereich Cloud-Computing. Im Allgemeinen sind Cloud-Dienste aufeinander angewiesen,

weil ihre einzelnen Strukturen auf einander aufgebaut sein können. So kann z.B. eine Verarbeitungscloud die Dienste einer Speicher-Cloud verwenden. Im Gegensatz zu lokalen Rechenzentren, die in einem einzelnen Land liegen, können sich solche Cloud-Infrastrukturen oft über mehrere Gerichtsbarkeiten und Länder erstrecken.

Deshalb hat die Frage des anwendbaren Rechts und des Schutzes der Verantwortlichkeiten des Benutzers bezüglich des Datenschutzes in länderübergreifenden Cloud-Szenarien Auswirkungen auf die Benutzung solcher Cloud-Dienstleistungen. Um eine unerwünschte Weitergabe von Daten zu verhindern, müssen ausreichende Schutzmechanismen eingerichtet werden. Diese können auch die Ebene der technischen Lösungen umfassen, wie z.B. Verschlüsselung, Datenminimierung oder die Durchsetzung von Datenverarbeitung



gemäß zuvor festgesetzter Richtlinien

Technische Ansätze in TClouds

Obwohl sich das Projekt noch in der Startphase befindet, zeichnen sich zwei komplementäre Stoßrichtungen und erste Ergebnisse ab, welche die verschiedenen Kompetenzen der Partner widerspiegeln. Zum einen ist dies die Ausgestaltung der Idee einer Cloud-of-Clouds, um auch bereits existierende Cloud Angebote abzusichern und zum anderen ist dies die Entwicklung einer eigenständigen sicheren Cloud-Infrastruktur. Beides erläutern wir im Folgenden beispielhaft. Abbildung 1 skizziert die TClouds Architektur. Die Cloud-of-Clouds Middleware integriert sowohl die neu entwickelte Trusted Cloud als auch Standard Cloud Angebote (Commodity Cloud) über den „Resiliency Layer“. Dadurch wird für

die Anwendungen eine einheitliche Schnittstelle angeboten.

Cloud-of-Clouds

Die Grundidee der Cloud-of-Clouds ist es, durch den gleichzeitigen Einsatz von Ressourcen und Diensten bei verschiedenen unabhängigen Cloud Anbietern sowohl die Sicherheit als auch die Zuverlässigkeit zu erhöhen. Ziel des Projektes ist es, hier die nötige Middleware zu schaffen um Dienste gemäß dieses Paradigmas zu verteilen und zu managen. Am Beispiel eines Speicherdienstes wurde dies mit dem DepSky Prototypen (Bessani, Correia, Quaresma, André, & Sousa, 2011) bereits umgesetzt. Durch die Replikation der Daten bei mehreren Anbietern bleiben die Daten auch dann verfügbar wenn einzelne Anbieter ausfallen (z.B. durch Denial-of-Service Attacken). Darüber hinaus ist das Protokoll so entwickelt, dass es auch sogenannte Byzantinische Fehler toleriert: Die Datenspeicherung funktioniert auch dann noch korrekt, wenn einzelne Clouds die Daten aktiv korrumpieren oder verlieren. Ganz pragmatisch vermindert eine Cloud-of-Cloud Infrastruktur, durch die Aufteilung der Ressourcen auf mehrere verschiedene Anbieter, auch die Gefahr des sog. „Vendor lock-in“, der Abhängigkeit des Anwenders von dem Angebot eines bestimmten Anbieters.

Trusted Clouds

Die wesentlichen Bausteine der in TClouds entwickelten „Trusted Cloud“ Infrastruktur, ist die Bereitstellung einer abgesicherten Ausführungsplattform (Betriebssystem und Hypervisor) für die virtuellen Maschinen der Kunden. Ein Baustein ist hier die Absicherung mittels Trusted Computing Technologien (Santos, 2009), welche die Integrität dieser Plattform für die Kunden überprüfbar macht.

Die zentrale Anforderung an die Ausführungsplattform ist das sichere Management der virtuellen Maschinen (VM) und die Einschränkung der Möglichkeiten eines Cloud-Administrators den Inhalt der virtuellen Maschinen zu lesen oder zu manipulieren.

Dazu werden zunächst alle Images der virtuellen Maschinen verschlüsselt abgelegt. Zur Ausführung einer VM müssen diese Images aber schließlich entschlüsselt werden, um die VM in den Speicher zu laden und auszuführen. Um

das Auslesen von vertraulichen Informationen aus dem Speicher zu verhindern muss die Plattform unerlaubten Zugriff auf den Speicher oder gar das Auslesen des kompletten Speicherinhaltes unterbinden. Ebenso muss die Migration einer VM, von einem physikalischen Server zu einem anderen, gegen Zugriffe abgesichert werden.

Hat man eine wie gerade skizzierte sichere Ausführungsplattform geschaffen gilt es für den Cloud Anbieter noch dem Kunden einen Nachweis zu liefern, dass diese Plattform auch eingesetzt wird. Dieser Nachweis kann durch den Einsatz Trusted Computing Technologie erfolgen. Durch das in der Hardware verankerte Trusted Platform Module (TPM) wird die Integrität der Plattform schon beim Booten geprüft und im TPM abgelegt und kann später sicher an den Kunden übermittelt werden.

Ein weiteres Ziel von TClouds ist die Integration von Trusted Virtual Domains (TVDs) (Catuogno, Löhr, Manulis, Sadeghi, & Stübli, 2010) in die Cloud Infrastruktur. Eine TVD benutzt Virtualisierung und Trusted Computing Technologie um auf gemeinsam genutzter Hardware isolierte virtuelle Domänen aufzubauen und TVD-weite Sicherheitsrichtlinien durchzusetzen. Typischerweise kapselt eine TVD einen Arbeitsablauf im Unternehmen, wie z.B. Management, Buchhaltung oder Entwicklung. Die Isolation der TVDs verhindert effektiv den ungewollten Informationsfluss zwischen verschiedenen TVDs. Das Konzept und die technischen Grundlagen für TVDs passen sehr gut zum Cloud Computing Paradigma, auch wenn der Fokus bislang eher auf hausinternen Lösungen lag. Daher soll das Konzept der TVDs um weitere Cloud Spezifika erweitert werden (z.B. die garantierte Trennung von verschiedenen Kunden auf verschiedenen physikalischen Rechnern). Desweiterensollen die Cloud Schnittstellen entsprechenden erweitert werden um eine nahtlose Integration von Cloud und Unternehmensinternen Ressourcen innerhalb von TVDs zu ermöglichen.

Ausblick

In diesem Beitrag haben wir einen Überblick über wichtige Sicherheits- und Datenschutzrisiken des Cloud Computing gegeben. Das EU Forschungsprojekt TClouds plant, diese sowohl durch die Absicherung einzelner Clouds als auch durch die

fehlertolerante Verbindung mehrerer Clouds in eine Cloud-of-Clouds zu mindern. Durch die Entwicklung einer sicheren Cloud-Infrastruktur wird so die Grundlage für die sichere und datenschutzkonforme Bereitstellung von Middleware und Anwendungen geschaffen.

Obwohl aktuelle Forschung Bausteine für die Absicherung der Cloud liefert, wird die Umsetzung in der Praxis erst erfolgen, wenn die Kunden vermehrt auch für kritische Unternehmensanwendungen Clouds einsetzen. Erst durch diesen Bedarf wird ein Markt für sichere Clouds geschaffen, welche die heutige Vorherrschaft von Clouds ohne Sicherheitsgarantien beenden wird.

Danksagungen

Wir danken dem TClouds Team für Anregungen und insbesondere den Autoren von (Glott et. al., 2011) für die Aufstellung zentraler Cloud Risiken. Unsere Forschung wird durch das TClouds Projekt (<http://www.tclouds-project.eu>) im Rahmen des siebten Forschungsprogramms der Europäischen Kommission gefördert (n°257243, FP7/2007-2013).

Literaturverzeichnis

- Bessani, A., Correia, M., Quaresma, B., André, F., & Sousa, P. (2011). DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. *EuroSys'11: The 6th ACM SIGOPS/EuroSys European Systems Conference*. Salzburg.
- Cabuk, S., Dalton, C.I., Eriksson, K., Kuhlmann, D., Ramasamy, H.V., Ramunno, G., Sadeghi, A.R., Schunter, M., Stübli, C. (2010): Towards automated security policy enforcement in multi-tenant virtual data centers. *J. Comput. Secur.* 18, 89–121.
- Catuogno, L., Löhr, H., Manulis, M., Sadeghi, A.-R., & Stübli, C. (5 2010). Trusted Virtual Domains: Color Your Network. *Datenschutz und Datensicherheit (DuD)*, S. 289-298.
- Chien, E (2010): W32.Stuxnet dossier. From <http://www.symantec.com/connect/blogs/w32stuxnet-dossier>, retrieved 2010-13-03
- Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J. (2009): Controlling data in the cloud: outsourcing computation with-

out outsourcing control. In: *ACM Workshop on Cloud Computing Security (CCSW'09)*. pp. 85–90. ACM Press

- Cloud Security Alliance (2010): Top threats to cloud computing, version 1.0. <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- Glott, Rüdiger, E.Husmann, A. Sadeghi, and Matthias Schunter (2011): Trustworthy Clouds underpinning the Future Internet, to appear in *Future Internet Assembly – Book 3*, Springer LNCS 6656
- Grobauer, B., Schreck, T. (2010): Towards incident handling in the cloud: challenges and approaches. In: *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*. pp. 77–86. CCSW '10, ACM, New York, NY, USA
- Kaliski, Jr., B.S., Pauley, W. (2010): Toward risk assessment as a service in cloud environments. In: *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*. pp. 13–13. HotCloud'10, USENIX Association, Berkeley, CA, USA,
- Organization for Economic Co-Operation and Development (2009): Guidelines on the protection of privacy and trans-border flows of personal data. From http://www.oecd.org/document/18/0,2340,en_2649_34255_18_15186_1_1_1_1,00.html (last modified January 5 1999), the OECD Privacy Principles
- Penn, J.: (2010): Security and the cloud: Looking at the opportunity beyond the obstacle. Forrester Research
- Rajan, S.S. (2010): Cloudsourcing vs outsourcing. Available online at <http://cloudcomputing.sys-con.com/node/1611752>
- Ristenpart, T., Tromer, E., Shacham, H., Savage, S. (2009): Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: *Proceedings of the 16th ACM conference on Computer and communications security*. pp. 199–212. CCS '09, ACM, New York, NY, USA
- Sadeghi, A.R., Schneider, T., Wnandy, M. (2010): Token-based cloud computing: secure outsourcing of data and arbitrary computations with lower latency. In: *Proceedings of the 3rd international conference on Trust and trustworthy comput-*

- ing, pp. 417–429. TRUST'10, Springer-Verlag, Berlin, Heidelberg
- Santos, N., Gummadi, K., & Rodrigues, R. (2009). Towards trusted cloud computing. *Proceedings of the 2009 conference on Hot topics in cloud computing*. Berkeley: USENIX Association.
- Santos, N., Gummadi, K.P., Rodrigues, R. (2009): Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing. pp. 3–3. Hot-Cloud'09, USENIX Association, Berkeley, CA, USA
- Vukolić, M. (2010): The byzantine empire in the intercloud. SIGACT News 41, 105–111
- Weichert, T. (2009): Cloud Computing und Datenschutz. Available online at <http://www.datenschutzzentrum.de/cloud-computing/>