Inter-Clouds: Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit

Gabi Dreo Rodosek[1], Mario Golling[1], Wolfgang Hommel[2],
Alexander Reinhold[1]

[1] Universität der Bundeswehr München, MNM-Team, Neubiberg
{gabi.dreo, mario.golling, alexander.reinhold}@unibw.de

[2] Leibniz-Rechenzentrum, MNM-Team, Garching
wolfgang.hommel@lrz.de

Abstract: Trotz der wirtschaftlichen Attraktivität und des unbestrittenen Marktpotentials gestaltet sich der Einsatz von Cloud-Computing in Deutschland weiterhin schwierig. Während auf der einen Seite gerade der Zusammenschluss von isolierten Cloud-Inseln zu Inter-Clouds („Cloud of Clouds“) verspricht, die unbestrittenen Vorteile des Cloud-Computing wie geringe Kosten durch effiziente, bedarfsgerechte Bereitstellung von Ressourcen noch weiter nach vorn zu treiben, sind Öffentlichkeit und Industrie durch die Vielzahl an Sicherheitsvorfällen der letzten Zeit für die Sicherheitsproblematik sensibilisiert worden. Dadurch rücken auch Sicherheitsfragen und -probleme beim Einsatz von Cloud-Computing stärker in den Fokus. Um daher den Unternehmen die sichere Nutzung der Inter-Clouds zu ermöglichen und nicht gegen den in Deutschland gültigen Datenschutz zu verstoßen, müssen zentrale Fragen wie Integrität, Vertraulichkeit, Nichtabstreitbarkeit, Transparenz, Authentizität und Verfügbarkeit adressiert werden. Als Basis für die Entwicklung geeigneter Sicherheitskonzepte, -methoden und -werkzeuge wird im Rahmen dieses Artikels ein Überblick über die Einsatzmöglichkeiten von Inter-Clouds sowie daraus resultierende Anforderungen an die IT-Sicherheit gegeben.

1 Einführung

Cloud-Computing verändert die Informations- und Kommunikationstechnologie (IKT) Landschaft zusehends. Die Vorteile des Cloud-Computing sind unbestritten. Neben dem flexiblen Zugriff auf Ressourcen (insbesondere bei Lastspitzen) ermöglicht Cloud-Computing auch eine schnellere Entwicklung neuartiger Anwendungen, Dienste und Lösungen, die besser an die Kundenwünsche angepasst sind. Gegen den breiteren Einsatz von Cloud-Computing spricht derzeit jedoch die mangelnde IT-Sicherheit. Ferner fordern die rechtlichen Bestimmungen hinsichtlich des Datenschutzes in Deutschland die Entwicklung neuer, eigener Cloud-basierter Lösungen.

Dadurch rücken die Sicherheitsfragen und -probleme beim Einsatz von Cloud-Computing besonders in den Fokus. Obligatorisch wird in diesem Themenkreis auch immer die Sicherheit der eigenen Unternehmensdaten genannt. Auch das Bundesdatenschutzgesetz (BDSG)

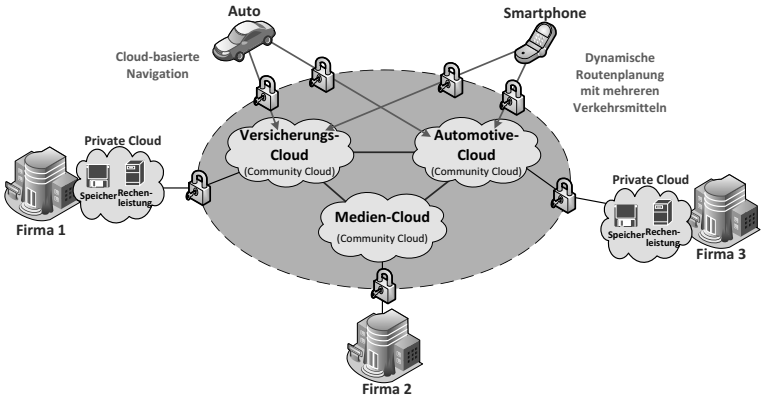

Abbildung 1: Sicherer Zusammenschluss von Clouds zu Inter-Clouds

in Deutschland stellt eine Hürde für den Einsatz von aktuellen Cloud-Computing Lösungen dar. Die großen Cloud-Computing Anbieter haben ihren Firmensitz ausschließlich in den USA und unterliegen damit dort geltenden Gesetzen, wie z. B. dem PATRIOT Act. Dieser erlaubt US-Behörden Zugriffe auf die bei den Cloud-Computing Anbietern gespeicherten Daten, ohne dass die betroffenen Kunden, d. h. die Eigentümer der Daten, informiert werden. Aus diesem Grund können deutsche Unternehmen solche Anbieter nur sehr eingeschränkt nutzen, ohne gegen die in Deutschland geltenden Datenschutzauflagen zu verstoßen.

Vint Cerf, der „Vater des Internets“, vergleicht das derzeitige Cloud-Computing mit der Zeit vor dem Internet, als versucht wurde, das ARPANET mit anderen Netzen zu verbinden (siehe auch: *Cloud-Computing and the Internet* von Vint Cerf[1]). Ähnlich wie das *Internet* der Zusammenschluss verschiedener Netze ist, ist auch die *Inter-Cloud* der Zusammenschluss verschiedener Clouds. Wie Abbildung 1 zeigt, bringt gerade der Zusammenschluss von Clouds zu Inter-Clouds den eigentlichen Mehrwert gegenüber isolierten Cloud-Inseln. Beispiele von Community Clouds sind die *Automotive-*, die *Versicherungs-*, die *Behörden-* oder die *Medien*-Cloud. Die Vernetzung von Community-Clouds ermöglicht es, Dienste und Daten aus einzelnen Community Clouds übergreifend zu innovativen Mehrwertdiensten zusammenzuführen sowie Cloud-übergreifend Ressourcen zu nutzen.

Die Voraussetzung für die sichere Vernetzung von Clouds in Inter-Clouds ist die Entwicklung einer IT-Sicherheitsarchitektur sowie die Entwicklung neuartiger Konzepte für die Datensicherheit. In diesem Beitrag werden die Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit in einer Inter-Cloud-Umgebung im Einklang mit der deutschen Rechtsprechung heraus gearbeitet.

[1] `http://googleresearch.blogspot.com/2009/04/cloud-computing-and-internet.html`

2 Terminologie

Um die Idee von Inter-Clouds veranschaulichen zu können, ist eine allgemeingültige Begriffsdefinition notwendig. Durch das National Institute for Standards and Technology (NIST) wurden im Bereich Cloud-Computing verschiedene Einsatzmodelle und Servicemodelle spezifiziert [MG11].

Die Einsatzmodelle *Public Cloud*, *Private Cloud* und *Community Cloud* unterscheiden sich hauptsächlich in der Art des Nutzerkreises der jeweilige Cloud. Bei einer Public Cloud ist der Nutzerkreis unbeschränkt, bei einer Private Cloud ist er auf ein einziges Unternehmen begrenzt. Community Clouds stellen eine zwischen verschiedenen Organisationen, die gemeinsame Interessen oder Vorgaben haben, geteilte Cloud-Infrastruktur dar.

Die Servicemodelle *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)* und *Software as a Service (SaaS)* variieren in der Art der angebotenen Dienste. IaaS-Dienste stellen dem Kunden selbst steuerbare hardwarenahe Ressourcen, wie z. B. Rechenkapazität und Speicherplatz, zur Verfügung, auf der er seine einige Software aufspielen und nutzen kann. PaaS-Dienste ermöglichen hingegen keine Kontrolle über die Cloud Infrastruktur, jedoch auf die Applikationsumgebung, wie z. B. dem Betriebssystem. Über die vom Provider angebotenen SaaS-Dienste können einzelne Applikationen genutzt werden; eine eigenständige Kontrolle der Cloud Infrastruktur oder eine Erweiterung um eigene Applikationen ist dabei nicht möglich.

3 Anwendungsbeispiele

In diesem Abschnitt wird die Notwendigkeit von Inter-Clouds anhand verschiedener Anwendungsfälle dargestellt. Sie wurden in enger Abstimmung mit Partnern aus der Wirtschaft erstellt und erheben somit einen Anspruch auf Realitätsnähe und Relevanz.

3.1 Inter-Cloud-basierte Navigation

Navigationsgeräte in Fahrzeugen sind weit verbreitet und führen Fahrer gut ans Ziel, indem sie das vorhandene Kartenmaterial und Eigenschaften von Verkehrswegen, z. B. Stau-Neigungen zu gewissen Uhrzeiten, auswerten und so eine möglichst gute Route vorschlagen. Aktuelle Informationen über die aktuelle Route betreffende Vorfälle können über Mobilfunk und auch per Traffic Message Channel (TMC) in die Planung aufgenommen werden, sind allerdings in ihrem Umfang limitiert. Auf Basis der Verknüpfung von Daten unterschiedlicher Quellen (bspw. intelligente Verkehrsführung, Unfallschwerpunkte, Baustellen, angemeldete Schwerlasttransporte und Straßenabsperrungen - siehe Abbildung 2) können noch komplexere Sachverhalte für Simulationen genutzt werden, die eine Berechnung von Strategien erlauben, um Staus noch effektiver zu verhindern oder abzumildern, Routen für Einsatzfahrzeuge frei zu machen oder das Risiko für Unfälle zu senken. Durch die Komplexität der notwendigen Berechnungen wird es aber erforderlich, Rechenkapazität

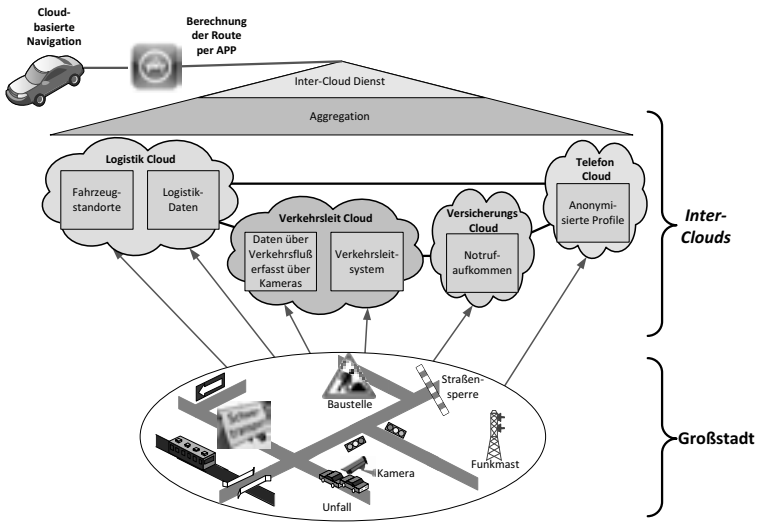

Abbildung 2: Zusammenführung von Daten unterschiedlicher Clouds zur Inter-Cloud-basierten Navigation

aus der Inter-Cloud zu nutzen, um eine zeitnahe Anpassung der Strategie erreichen zu können. So kann z. B. diese Anwendung einem sich im Stau befindenden Pendler den Weg zum nächsten Park-and-Ride-Parkplatz weisen und ihn über die öffentlichen Verkehrsmittel zu seinem Ziel lotsen, oder einen Studenten über eine Stellwerksstörung informieren und ihn zum nächsten Leihfahrrad führen.

3.2 Inter-Cloud in der öffentlichen Verwaltung

Cloud-Computing ist für die kommunale Verwaltung eine attraktive Lösung, um einfach Infrastruktur-Ressourcen (IaaS) bei Lastspitzen zuzuschalten oder Anwendungsdienste (SaaS) mit anderen Kommunen zu teilen. Während für die reine Datenspeicherung Verschlüsselungslösungen existieren, muss die Verarbeitung der Daten bis auf absehbare Zeit noch unverschlüsselt erfolgen und ist damit prinzipiell unsicher. Mit einer Klassifizierung von Daten und der Möglichkeit der Weiterverarbeitung in der Inter-Cloud können Ressourcen, die nur bei Spitzenlast gebraucht werden, aus der Inter-Cloud bezogen werden. Sensible Daten müssen hierzu pseudonymisiert werden.

Dazu muss ein generischer Dienst zur Verfügung gestellt werden, der es erlaubt, Informationen unter Berücksichtigung der Bedürfnisse der Anwender mittels Pseudonymisierung in der Inter-Cloud zu verarbeiten, wobei die zu verarbeitenden Daten unterschiedlichen Schutzbedarf haben können. Abhängig davon können bspw. Daten ausschließlich in einer Private Cloud, in einer Inter Community Cloud eines vertrauenswürdigen Partners oder in einer Public Cloud verarbeitet werden. Die vertraulichen Daten der Anwender werden

dabei stets ausschließlich in der Datenbank der Behörde gespeichert und verlassen deren Private Cloud nicht.

3.3 Inter-Cloud in der Gebäudeautomatisierung

In modernen Gebäudeautomatisierungssystemen werden permanent Sensordaten unterschiedlicher Betreiber produziert, die auf geeignete Weise ausgewertet, korreliert, protokolliert und gespeichert werden müssen, etwa Bildmaterial in Videoüberwachungssystemen, Raumluftparameter wie Temperatur und Rauchkonzentration in Brandmeldesystemen, oder Daten von Bewegungsmeldern einer Einbruchsmeldeanlage. In traditionellen Systemen werden die entstehenden Daten direkt auf den Geräten bzw. auf Zentraleinheiten im Gebäude verarbeitet und gespeichert. Durch zunehmende Netz- und Internetfähigkeit der Geräte wird es möglich, Funktionalität und Speicherkapazität nicht mehr ausschließlich lokal vorzuhalten, sondern selektiv auszulagern. Solche Systeme sind insbesondere in kleinen und mittelständischen Unternehmen (etwa Tankstellen, Bekleidungseinzelhandel, Cafés) attraktiv, weil sich so Funktionen kostengünstig bereitstellen lassen und die Fähigkeiten mit den Anforderungen dynamisch wachsen können.

Inter-Cloud-Dienste können dabei für die Analyse von Sensordaten, etwa zur Erkennung von Alarmfällen (Feueralarm, Einbruchsalarm), zur Optimierung von Heizungs-, Belüftungs- und Beleuchtungssystemen, oder zur Unterstützung von Business Analytics (z. B. Reduzierung von Wartezeiten an Kassen und Beratungspunkten) genutzt werden.

4 Anforderungsanalyse

Bereits aus den drei oben stehenden Anwendungsszenarien ergeben sich eine Vielzahl offensichtlicher Anforderungen. Vor allem die gesetzlichen Vorgaben des BDSG beeinflussen diese stark. Durch die Kumulation der Daten könnten Cloud-Anwendungen die Erstellung von personifizierten Bewegungs- und Nutzungsprofilen forcieren. Um die Persönlichkeitsrechte jedes Einzelnen zu wahren, sind Methoden zu bewerten und zu entwickeln, die die Daten soweit möglich in anonymisierter bzw. pseudonymisierter Form verarbeiten. Speziell bei der Zusammenführung von Datenbeständen unterschiedlicher Behörden stellt dies eine große Herausforderung dar, da hier unter Umständen der Personenbezug bestehen bleiben muss. Durch technische Maßnahmen muss in solchen Fällen die Verarbeitung personenbezogener Daten unter Einhaltung geltenden (deutschen) Rechts gewährleistet sein.

Zudem ist die Datensicherheit bei der Nutzung einer Inter-Cloud speziell für sensible Daten zu garantieren. Die technische Umsetzung hat sowohl die sichere Datenspeicherung und -verarbeitung als auch den sicheren Datentransport zu umfassen. Anhand von zu spezifizierenden Datenschutzklassen kann das Sicherheitsniveau für Daten festgelegt werden. In Abhängigkeit der Schutzklassen kommen unterschiedlich ausgeprägte Sicherheitsmechanismen zur Anwendung. Existierende Protokolle im Bereich Cloud-Computing können als Basis dienen und sind um die Zuordnung von Daten zu bestimmten Schutzklassen zu erwei-

tern. Die Robustheit und Verfügbarkeit von Daten und Diensten sind durch vorzuhaltende Mechanismen auch im Katastrophenfall sicherzustellen.

Der Verbund einzelner Clouds miteinander setzt gegenseitiges, verifizierbares Vertrauen der Kooperationspartner und somit ein Trust Management System voraus. Anhand von festzulegenden, objektiven Kennzahlen ist eine Klassifizierung von den beteiligten Providern als auch von den einzelnen Cloud Diensteanbietern vorzunehmen. In Abhängigkeit von den unterstützten Verfahren zur Gewährleistung der Sicherheit (Authentifizierungsverfahren, Verschlüsselungsmechanismen, Verfügbarkeit, Integrität etc.) und auf Basis der Reputation kann z. B. eine Klassifizierung vorgenommen werden.

Der sichere, organisationsübergreifende Ansatz, Daten über eine Inter-Cloud-basierte Infrastruktur miteinander auszutauschen und diese gemeinsam zu nutzen, erfordert eine organisationsübergreifende Authentifizierungs- und Autorisierungsinfrastruktur (AAI). Daraus ergibt sich zudem die Notwendigkeit eines föderierten Identitätsmanagements (FIM) für Inter-Cloud-Umgebungen.

Inter-Clouds beherbergen zum einen eine hohe Anzahl an nutzbaren, ggf. äußerst sensiblen und personifizierten Daten, zum anderen stellen sie ein hohes Maß an verteilten Ressourcen bereit. Allein durch die beiden Punkte ergeben sich neue Angriffsvektoren und Missbrauchsmöglichkeiten, die es genauer zu identifizieren gilt. Nach einhergehender Analyse und Bewertung dieser Bedrohungen sind entsprechende Verfahren zu entwickeln bzw. existierende in das Cloud Umfeld zu portieren. Dies können z. B. speziell ausgelegte, organisationsübergreifende Intrusion Detection Systeme sein.

Für alle Mechanismen, Verfahren und Prozesse für die Speicherung, Verarbeitung und für den Transport der Daten im Inter-Cloud Umfeld gilt, dass sie auditier- und verifizierbar sein müssen, um ein hohes Maß an Sicherheit und Vertrauen zu gewährleisten.

5 Analyse des Stands der Wissenschaft und Technik

Durch seine grundlegende Bedeutung für den Einsatz von Rechen- und Speicherressourcen und durch das große Marktpotenzial bedingt wird Cloud-Computing derzeit im Rahmen vieler industrieller Gremien, wissenschaftlicher Arbeiten, Studien und Projekte unter verschiedensten Blickwinkeln untersucht. Im Folgenden fassen wir eine Analyse ausgewählter Cloud-Sicherheitseigenschaften im Kontext von Inter-Clouds zusammen, um die aktuellen Möglichkeiten und Grenzen des Stands von Wissenschaft und Technik aufzuzeigen. Hierzu betrachten wir im Folgenden zunächst die aktuelle Literatur zu diesem Thema und zeigen im Anschluss eine Gegenüberstellung aktueller deutscher Cloud-Projekte.

5.1 Studien und wissenschaftliche Beiträge zur Cloud-Sicherheit

Zu den bekanntesten europäischen Studien zum Cloud-Computing gehören diejenigen der ENISA [CH09] und des Fraunhofer AISEC [SR09]. Sie betrachten die Thematik primär aus

Perspektive der Cloud-Computing-Nutzer. In den Arbeiten des BSI [Bun11] wurden komplementär dazu die Mindestsicherheitsanforderungen an Cloud-Computing-Dienstleister erarbeitet. Dabei wurden Technologien und Prozesse spezifiziert, die von Cloud-Computing-Dienstleistern umzusetzen sind. Auch das US-amerikanische NIST verfolgt das Ziel intensiv, gemeinsam mit der Industrie neue Standards zu entwickeln und Lösungen u. a. für Cloud-Interoperabilität, Portabilität und Sicherheit zu erforschen. Ferner definiert auch die Cloud Security Aliance mit der Cloud Security Alliance Cloud Controls Matrix (CCM, [Clo]) u. a. die Sicherheitsgrundsätze für Cloud-Dienstleister, um Sicherheitsrisiken besser abschätzen zu können. Die CCM bietet hierzu einen Rahmen für ein detailliertes Verständnis von Sicherheitskonzepten und Grundsätzen für Cloud-Security-Standards und zeigt die Beziehungen zu anderen Sicherheitsstandards, Vorschriften und Kontroll-Frameworks (u. a. ISO 27001, COBIT) auf. Das Global Inter-Cloud Technology Forum (GICTF) fördert die weltweite Standardisierung von Inter-Cloud-Systemschnittstellen zur Gewährleistung der Interoperabilität; ein Schwerpunkt ist die garantierte Verfügbarkeit von Diensten bei partiellem Systemausfall innerhalb einer Inter-Cloud-Umgebung [Glo10].

Diverse auch für Inter-Clouds relevante Sicherheitsprobleme sind schon in anderen Zusammenhängen umfassend behandelt worden, wie beispielsweise der sichere Datentransfer [KS05] und das sichere Datenbackup mit Hilfe von Verschlüsselung. Mehrere Forschungsvorhaben, z. B. [RTSS09], beschäftigen sich mit der Sicherheit der eingesetzten Virtualisierungstechniken. Ferner beschäftigen sich die Trusted Cloud Initiative der Cloud Security Alliance OASIS [OAS] und die Open Identity Exchange Initiative mit der sicheren Identitäts- und Rechteverwaltung im Rahmen des Cloud-Computing. In diesem Zusammenhang richten die wissenschaftlichen Arbeiten von Bertino et al. [BPFS09] und Huang et al. [HZH09] besonderes Augenmerk auf den Schutz der personenbezogenen Daten der Nutzer von Cloud Services. Celesti et al. spezifizieren die Referenzarchitektur ICIMI (InterCloud Identity Management Infrastructure), die das Problem des Identitätsmanagements in Inter-Clouds angeht [CTVP10].

5.2 Gegenüberstellung aktueller deutscher Cloud-Projekte unter Sicherheitsgesichtspunkten

Eine inzwischen recht große Zahl deutscher, zum Teil geförderter Projekte thematisiert Cloud-Computing und setzt sich dabei überwiegend explizit mit Sicherheitsaspekten auseinander. Im Folgenden konzentrieren wir uns aus Platzgründen auf solche Projekte, die mehrere Aspekte der Cloud-Sicherheit parallel in Angriff nehmen; darüber hinaus existieren zahlreiche weitere Projekte, die sich mit ausgewählten Basistechnologien wie dem Identity Management im Cloud-Umfeld auseinandersetzen.

Zu den hier betrachteten Projekten gehören im Rahmen des BMWi-Programms Trusted Cloud die Projekte CloudCycle, Value4Cloud, Sealed Cloud, SkIDentity, MIA, Cloud4E, Peer Energy Cloud, Sensor Cloud und goBerlin. Das Projekt Mimo Secco thematisiert Cloud Security im Kontext mobiler Dienstnutzung. Sec2 vertieft den Anwendungsfall Ad-hoc On Demand Virtual Private Storage. Die CollabCloud legt ihren Schwerpunkt auf Dokumentenmanagement und kombiniert Data Mining und Semantic Computing mit

Clouds. Frankfurt und Berlin haben eigene städtespezifische Cloud-Projekte; während in Berlin das Ziel Open Data im Vordergrund steht, spezialisiert sich die Frankfurt Cloud auf die Unterstützung rechen- und datenintensiver Forschungsvorhaben. Die deutsche Anteil der Eurocloud wird vom Verband der deutschen Cloud-Computing-Industrie betrieben; eine Kompetenzgruppe Recht und Compliance setzt sich dabei mit Regelungen um Datenlokationen, Archivierungsvorgaben, Abrechnungsverfahren und Eigentumsverhältnissen auseinander.

Im Rahmen des Projekts mOSAIC werden Vermittlungsdienste auf Basis einer Open Source API entwickelt. BonFIRE bietet hingegen eine kommerziell angebotete Cloud-Infrastruktur, die insbesondere räumlich verteilte Ressourcen zu einem Ganzen bündeln kann. Im Projekt VENUS-C wird eine Plattform für die Entwicklung und Forschung rund um Cloud-Services erarbeitet; StratusLab fokussiert IaaS-Plattformen auf Open-Source-Basis und erarbeitet Methoden zur einfachen Integration weiterer Ressourcen. Die Deutsche Wolke ist schließlich eine Initiative zum Aufbau einer föderierten Cloud-Infrastruktur in Deutschland auf Basis offener Standards und Open Source.

Die sicherheitsspezifischen Gemeinsamkeiten und Unterschiede dieser Projekte sind in Abbildung 3 dargestellt. Betrachtet werden dabei zum einen Datenschutzaspekte, d.h. ob personenbezogene Daten verarbeitet werden, ob bewusst Nutzungsprofile erstellt werden, ob Geheimhaltungsvereinbarungen im Rahmen industrieller Anwendungen vorgesehen sind, ob die Konformität mit dem Bundesdatenschutzgesetz explizit thematisiert wird und inwiefern eine anonymisierte Datenverarbeitung vorgesehen ist. Ferner wird betrachtet, ob die Nutzung standardisierter Protokolle vorgesehen ist und ob explizite Konzepte für die Authentifizierung, Autorisierung und das Trust Level Management existieren. Neben der einfachen Erweiterbarkeit um neue Dienste und die Berücksichtigung betriebswirtschaftlicher und rechtlicher Anforderungen werden auch die praktische Umsetzung, z. B. in Form eines Demonstrators, betrachtet.

Insgesamt zeigt sich, dass Aspekte wie die Definition und forcierte Umsetzung von Schutzklassen für Daten, die Berücksichtigung benutzerfreundlicher Sicherheitsmechanismen z. B. durch Single Sign-On, explizites Cloud-Risikomanagement, der Einsatz quantifizierender Sicherheitskennzahlen und die Zusammenarbeit mit Standardisierungsgremien noch verstärkt angegangen werden müssen. Auch die Aktivitäten im Inter-Cloud-Bereich müssen noch deutlich ausgebaut werden.

6 Zusammenfassung

Um den Unternehmen in Deutschland die sichere Nutzung des Cloud/Inter-Cloud-Computing bei gleichzeitiger Wahrung der wirtschaftlichen Vorteile desselben zu ermöglichen, bedarf es insbesondere einer ganzheitlichen IT-Sicherheitsarchitektur, die im Idealfall bereits zum Zeitpunkt des Designs integraler Bestandteil des Gesamtkonzepts ist („Security by Design"). Diese hohe Bedeutung der IT-Sicherheit für das Thema Cloud-Computing verdeutlichen u. a. die zahlreichen Förderprojekte auf nationaler und Internationaler Ebene, wie das Aktionsprogramm Cloud-Computing, die Hightech-Strategie 2020 für Deutschland

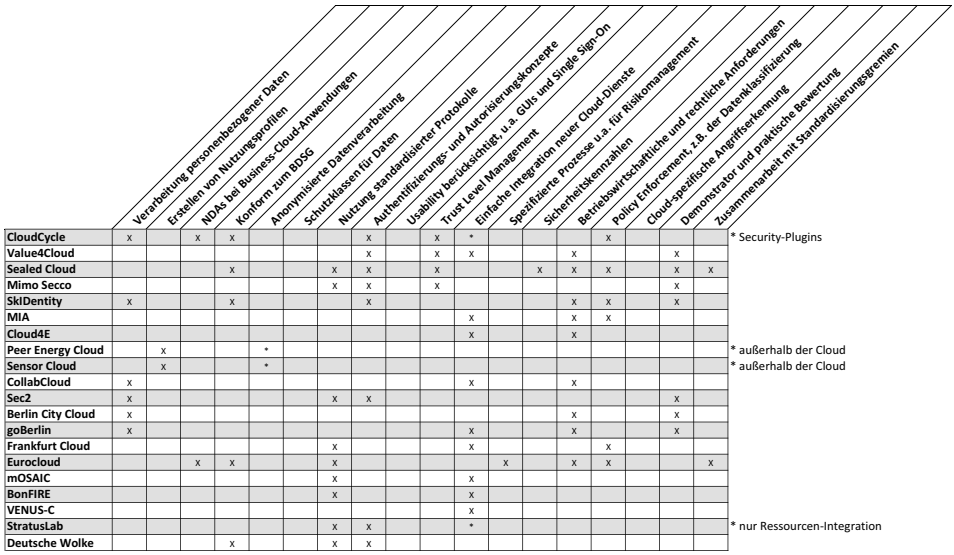

Abbildung 3: Gegenüberstellung laufender deutscher Cloud-Projekte unter Sicherheitsaspekten

oder die EU-Strategie zum Cloud-Computing.

Mit dem Ziel, Anforderungen an eine sichere Inter-Cloud-Lösung abzuleiten, wurden im Rahmen dieses Artikels in enger Kooperation mit Anwendern wie BMW, Allianz und der Landeshauptstadt München unterschiedliche Anwendungsfälle und Szenarien erarbeitet, aus denen Anforderungen an eine sichere Inter-Cloud-Lösung abgeleitet wurden. Um als Ziel diese innovativen, sicheren Inter-Cloud-basierten Mehrwertdienste in einer sicheren und vertrauenswürdigen Umgebung zu realisieren, bedarf es darauf aufbauender IT-Sicherheitskonzepte, -methoden, -prozesse und -werkzeuge, die es ermöglichen, Inter-Clouds in der gewünschten Weise sicher zu nutzen. Dazu müssen u. a. Antworten auf folgende Problemfelder gefunden werden:

- Festlegung einer Sicherheitstaxonomie
- Definition einer sicheren Inter-Cloud-Kommunikation
- Inter-Cloud Identity Management
- Angriffserkennung in einer Inter-Cloud-Umgebung
- Spezifikation von Sicherheitsmangementprozessen

In weiterführenden Forschungsarbeiten werden wir zunächst den Fokus auf die Aspekte der Datenkorrelation und Verdichtung sowie der Angriffserkennung in Inter-Clouds legen.

Danksagung

Die Autoren danken dem Munich Network Management Team (LMU, LRZ, UniBwM), den Mitarbeitern von Fraunhofer AISEC sowie Mitarbeitern von Bosch Sicherheitssysteme, Giesecke&Devrient, Infineon, SpaceNet AG, EURO-LOG, SSP Europe, Telefonica, Oracle, BMW, Allianz und der Landeshauptstadt München für wertvolle Hinweise und Diskussionen.

Literatur

[BPFS09] E. Bertino, F. Paci, R. Ferrini und N. Shang. Privacy preserving digital identity management for Cloud-Computing. *IEEE Data Eng. Bull.*, 32(1):21–27, 2009.

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. *Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit)*. Bundesamt für Sicherheit in der Informationstechnik, 2011.

[CH09] D. Catteddu und G. Hogben, Herausgeber. *Cloud Computing – Benefits, risks and recommendations for information security*. The European Network and Information Security Agency (ENISA), 2009.

[Clo] Cloud Security Alliance. Cloud Controls Matrix V1.1. `https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/`.

[CTVP10] A. Celesti, F. Tusa, M. Villari und A. Puliafito. Security and Cloud Computing: Inter-Cloud Identity Management Infrastructure. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, pages 263 –265, june 2010.

[Glo10] Global Inter-Cloud Technology Forum. Use Cases and Functional Requirements for Inter-Cloud Computing. `http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf`, 2010.

[HZH09] X. Huang, T. Zhang und Y. Hou. ID management among clouds. *First International Conference on Future Information Networks (ICFIN)*, pages 241–273, 2009.

[KS05] S. Kent und K. Seo. Security Architecture for the Internet Protocol. *Network Working Group, Request for Comments: 4301*, 2005.

[MG11] P. Mell und T. Grance. The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, 800-145:7, 2011.

[OAS] OASIS. OASIS Identity in the Cloud TC. `http://www.oasis-open.org/committees/tc_home.php`.

[RTSS09] T. Ristenpart, E. Tromer, H. Shacham und S. Savage. Hey, you, get off of my cloud: Exploring Information Leakage In Thirdparty Compute Clouds. *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 199–212, 2009.

[SR09] W. Streitberger und A. Ruppel. *Cloud Computing Sicherheit – Schutzziele. Taxonomie. Markübersicht.* Fraunhofer SIT, 2009.