Sicherheit und rechtliche Herausforderungen in Bezug auf Cloud Computing und Kritische Infrastruktur-IT

M. Tauber, Ch. Wagner, F. Pallas[1]

Die Machine-to-Machine (M2M) Kommunikation nimmt durch die Vernetzung von Diensten und Geräten, wie sie zum Betrieb von kritischen Infrastrukturen (z. B. „smart-grids“, intelligente Verkehrssteuerung und Überwachungssysteme) notwendig ist, laufend zu. Daraus resultiert ein sich stetig erhöhender Bedarf an Speicherplatz und Rechenleistung. Die Geräte im Feldeinsatz verfügen über limitierte Ressourcen, und oft ist auch eine globale Sicht auf Daten von mehreren Geräten notwendig. Der natürliche Ansatz ist daher, Daten und deren Verarbeitung in „die Cloud“ auszulagern. Dadurch ergeben sich allerdings Herausforderungen in den Bereichen Sicherheit, Datenschutz und im Hinblick auf die Verbindung dieser technischen Herausforderungen mit rechtlichen Aspekten. Dieser Artikel erklärt Ansätze und Motivation zur Untersuchung dieser Themen im Umfeld von kritischen Infrastrukturen, Cloud und M2M Kontext.

Schlüsselwörter: Sicherheit; Datenschutz; Cloud; M2M; kritische Infrastruktur-IT

Security and legal Challenges in Cloud Computing and critical Infrastructure IT.

The prevalence of machine-to-machine (M2M) will continue to increase because of the connection and interlinking of services in the domain of critical infrastructures (e. g. “smart grids”, traffic management or surveillance systems). This is leading to a constant rise of required computational and storage resources. As field systems typically offer only limited computing and storage capabilities and as many applications require a global view to integrated data from various devices, a natural location to store data and perform analysis tasks is in the Cloud, where an abundance of flexible resources can be used. However, this results in a number of security and privacy challenges in combination with some legal and technical considerations that need to be addressed. In this paper, we will investigate and categorize the above challenges associated with using the Cloud in a critical infrastructure and M2M context.

Keywords: Security, Data protection, Cloud, M2M, critical infrastructure IT

Eingegangen am 26. Juli 2013, angenommen am 29. August 2013

1. Einleitung und Problemstellung

Kritische Infrastrukturen gewährleisten, dass die Grundbedürfnisse des modernen Menschen befriedigt werden können. Dies beinhaltet Stromnetze, Wasserversorgung, Verkehrskontrollsysteme,

[1] **Tauber, Markus**, AIT Austrian Institute of Technology GmbH, 2444 Seibersdorf, Österreich (E-Mail: markus.tauber@ait.ac.at); **Wagner, Christian**, AIT Austrian Institute of Technology GmbH, 2444 Seibersdorf, Österreich; **Pallas, Frank**, Karlsruher Institut für Technologie (KIT), Zentrum für Angewandte Rechtswissenschaften (ZAR), Kaiserstraße 12, 76131 Karlsruhe, Deutschland

das Internet oder auch, so kontrovers das Thema auch ist, Überwachungssysteme (z. B. CCTV), die der Aufrechterhaltung der öffentlichen Ordnung dienen. Moderne IT-Systeme für die Steuerung solcher kritischer Infrastrukturen erlauben dabei eine Steigerung der Effizienz und verringern die Notwendigkeit zur (bislang oftmals praktizierten) Überdimensionierung eben dieser Infrastrukturen. Solche Steuerungselemente bzw. Systeme sind klassische Anwendungsfelder in der Machine-to-Machine (M2M) Kommunikation. Die Nutzung solcher Ansätze der M2M Kommunikation im Anwendungsfeld kritischer Infrastrukturen erlaubt außerdem das Managen von nicht vorhersehbaren lokalen Spitzenlasten. Die Verwendung entsprechender Systeme findet daher auch im Bereich der kritischen Infrastrukturen zunehmend Anklang. Störungen durch z. B. gezielte Einbringung von Schadsoftware in die Steuerung solcher Systeme können allerdings fatale Folgen haben (Peerenboom et al., 2001) und müssen daher weitest möglich vermieden werden.

Die von Steuerungs- und Kontrollgeräten für kritische Infrastrukturen im Feldeinsatz gelieferten Daten müssen zudem in vielen Anwendungsfällen zu einer globaleren Sicht integriert werden, um sich überhaupt sinnvoll nutzen zu lassen. Gleichzeitig verfügen die Feldgeräte jedoch meist nur über limitierte Ressourcen. Der natürliche Ansatz ist daher Daten und Verarbeitung auch im Kontext kritischer Infrastrukturen in die Cloud auszulagern. Mit einer der Hauptgründe dafür sind die schwer vorhersehbaren punktuellen Spitzenlasten in kritischen Infrastrukturen, da hier von der dynamischen Ressourcenzuordnung in der Cloud profitiert werden können. Übertragen auf die M2M Kommunikationsterminologie bedeutet dies, dass die Cloud den Datenintegrationspunkt (DIP) und z. B. smart-meter oder CCTV-Kommunikations-Schnittstellen Datenendpunkte (DEP) darstellen.

Traditionelle Ansätze in der IT zur Absicherung von Infrastrukturen können in diesem Zusammenhang jedoch unter Umständen nicht angewandt werden. Grund dafür ist, dass kritische Infrastrukturen historisch – im Unterschied zu traditionellen IT-Infrastrukturen – als isolierte Netzwerke betrachtet werden und wie o. g. (Supervisory Control and Data Acquisition (SCADA)-) Komponenten oft nur über limitierte Ressourcen verfügen. Dieser Artikel stellt die sich dadurch ergebenden Herausforderungen vor und skizziert, wie sie im EU/FP7 Projekt SECCRIT (SEcure Cloud computing for CRitical Infrastructure IT) adressiert werden.[2] Die Themen beinhalten insbesondere die Kombination von technischen und rechtlichen Aspekten, Risikobewertung, Anomalie-Erkennung und „Assurance“. Im Folgenden wird die Relevanz dieser Themen u. a. anhand eines SECCRIT Demonstrator-Beispiels dargestellt. Darüber hinaus wird skizziert, wie die sich daraus ergebenden Fragen und Herausforderungen im Rahmen des Projekts SECCRIT von einem breiten Konsortium aus Bedarfsträgern und Experten adressiert werden.

2. Hintergrund und Relevante Literatur

In der Untersuchung von verwandten Themenstellungen (Peerenboom et al., 2001) wird zwar die gegenseitigen Störungen kritischer Infrastrukturen eingegangen und deren fatale Auswirkungen diskutiert, aber es wird nicht detailliert aufgezeigt, dass bzw. wie die in Kapitel 1 genannten Themen behandelt werden sollten.

Iankoulova et al. (2012) geben Empfehlungen von zu behandelnden Themen ab und kategorisieren und priorisieren diese. Es wird auch erläutert, welche Sicherheitsanforderungen in der Literatur bereits eingehend behandelt wurden. Hierbei zeigt sich, dass unter anderem Aspekte der Service-Widerherstellung nach Problemen sowie rechtliche Fragen noch nicht ausreichend erforscht sind.

Eine gewichtete Liste von Bedrohungen für Cloud Computing wird in einem 2010 herausgegebenen Artikel der Cloud Security Alliance aufgezeigt (Cloud Security Alliance, 2010), wobei dieser aber auf

[2] Für mehr Infos über SECCRIT siehe – www.seccrit.eu

kritische Infrastrukturen im Detail nicht eingeht. Catteddu et al. liefern im 2009 publizierten ENISA-Bericht einen Kriterienkatalog (Catteddu et al. 2009), der bei der Auswahl eines Cloud-Anbieters helfen soll, gehen aber nicht auf die Entwicklung von Gegenmaßnahmen oder die Bedürfnisse von kritischen Infrastrukturen ein. Den Besonderheiten der im Rahmen des Projekts SECCRIT untersuchten Szenarien im Kontext kritischer Infrastrukturen tragen die genannten Berichte ebenfalls nicht ausreichend Rechnung. Die Risikolage eines Cloud-Services zu analysieren ist zudem – verglichen mit traditionellen Lösungsansätzen (Burton et al., 2010) komplexer und mehrdimensionaler und erfordert daher dedizierte Untersuchungen. Dekker legt im 2012 erschienenen Bericht der European Network and Information Security Agency (ENISA) erste Empfehlungen zur Risikoanalyse und Risikobewertung im Bereich des Cloud Computings dar (Dekker et al., 2012). In beiden Fällen wird jedoch keine klare Vorgehensweise aufgezeigt. Entsprechende Risikobewertungsmethoden mit explizitem Fokus auf Cloud Computing in kritischen Infrastrukturen werden daher im Rahmen des Projekts SECCRIT ebenfalls erforscht.

Ähnliches gilt für den Bereich der gerade im Kontext kritischer Infrastrukturen besonders relevanten Technologien zur Anomalie-Erkennung (Chandola et al., 2009). Durch das dynamische Verteilen von Netzwerklasten in Cloud-Umgebungen können etablierte Technologien zur Anomalie-Erkennung schnell an ihre Grenzen stoßen und sich damit für die im Projekt SECCRIT untersuchten Anwendungsfälle als untauglich erweisen. Auch hier sollen im Rahmen des Projekts neue Ansätze und Vorgehensweisen entwickelt werden, die letztendlich nicht nur im Bereich kritischer Infrastrukturen zum Einsatz kommen können.

3. Herausforderungen und Untersuchungsansätze im Einsatz von Cloud als DIP Technologie im kritischen Infrastruktur Bereich

Die Ziele des SECCRIT Projekts lassen sich am besten auf Basis eines Use-Cases illustrieren. So legen wir im Rahmen von SECCRIT unter anderem den Anwendungsfall eines Cloud-basierten Videoüberwachungssystems für eine fiktive U-Bahn Station zugrunde, den wir mit unserem Demo-Partner Mirasys[3] in Finnland unter möglichst realen Bedingungen nachbilden. Bildanalysesoftware und Speicherplatz werden hier zur Performancesteigerung und zur besseren Ressourcennutzung in die Cloud ausgelagert, da einige Funktionalitäten nur unter bestimmten Bedingungen benötigt werden. So kann beispielsweise eine rechenintensive automatische Bild- bzw. Situationsanalyse zur Vandalismus-Vermeidung nur dann erforderlich sein, wenn zuvor erkannt wurde, dass sich während nächtlicher Schließzeiten Personen in der Station aufhalten. Zur Bewältigung solcher, nur vereinzelt auftretender Spitzenlasten müsste ohne Cloud Computing lokale Rechenkapazität vorgehalten werden, die die meiste Zeit ungenutzt bleibt. Eine dynamische Zuschaltung von Ressourcen, wie sie die Cloud bietet, erscheint demgegenüber zweifellos vorteilhaft. Mit der Auslagerung von Rechen- und Speicherkapazität kann dabei auch die Auslagerung von Teilen des Services einhergehen – zum Beispiel das Management und der technische Betrieb der einzelnen Überwachungskameras sowie deren Integration in ein Gesamtsystem auf Basis einer entsprechenden Software as a Service (SaaS)-Lösung.

Herausforderungen, die im Rahmen des SECCRIT-Projektes – repräsentativ für ähnliche Anwendungsfälle – behandelt werden, ergeben sich beispielsweise aus fiktiven Situationen, in denen (1) kompromittierendes Bildmaterial an Dritte weitergegeben wird oder (2) in denen die „cloudifizierte“ Überwachungs- und Analysesoftware einen größeren Vandalismus-Akt nicht an den Sicherheitsdienst meldet.

[3] Ein CCTV-Technologie Provider und Mitglied des SECCRIT Konsortiums (www.seccrit.eu)

SECCRIT Forschungsthemen und angestrebte Anwendung der Ergebnisse:

- Verknüpfung von rechtlichen und technischen Aspekten – Aus den im Rahmen von SECCRIT betrachteten Anwendungsfällen ergibt sich eine Vielzahl rechtlicher Rahmenbedingungen und Fragestellungen, denen die technischen Modelle und Verfahren Rechnung tragen müssen. So stellt sich beispielsweise die Frage, unter welchen Bedingungen die Nutzung des Cloud Computings im Kontext kritischer Infrastrukturen z. B. datenschutzrechtlich überhaupt zulässig ist bzw. welche Cloud-spezifischen Anforderungen sich in diesem Bereich ergeben. Außerdem sollen im Projekt technische Verfahren entwickelt werden, auf deren Basis sich mit ausreichender rechtlicher Beweiskraft z. B. in obiger Situation (1) das „Leak" identifizieren lässt oder obiger Situation (2) haftungsrelevante Informationen zur Verantwortlichkeit für die Fehlfunktion des Gesamtsystems erfasst werden können. Die zur Beantwortung dieser und ähnlicher Fragen erforderliche enge Integration rechtlicher und technischer Aspekte ist eines der Kernkonzepte des Projekts SECCRIT.

- Anomalie-Erkennung & Root Cause Analysis – War z. B. in Situation (2) die Nichtmeldung an den Sicherheitsdienst das Resultat einer gezielten Cyberattacke gegen das „cloudifizierte" System? SECCRIT Tools & Methoden sollen hier helfen dies zu erkennen. Anomalie-Erkennung ist eine Kombination verschiedenster Techniken, die helfen unerwartetes Verhalten von Komponenten der kritischen Infrastruktur zu erkennen und zu evaluieren ob dieses Verhalten durch einen Angriff ausgelöst wurde. Dies beinhaltet die Definition von zu überwachenden Attributen des Systems und das Lernen ab wann die überwachten Attribute auf einen Angriff schließen lassen können. In Cloud-Umgebungen, in denen dynamisch Ressourcen zu- oder weggeschalten werden können, ist es darum eine Herausforderung unzulässig verbrauchte Ressourcen zu identifizieren. Im Rahmen des Projekts SECCRIT wird untersucht inwieweit etablierte Anomalie-Erkennungssysteme im Cloud- und kritischen Infrastruktur Bereich angewendet werden können und an welchen Punkten in der System-Architektur hierzu welche Informationen gesammelt werden können (Monitoring).

- Risikobewertungsmethoden und Risikokataloge – z. B. zur Priorisierung der Entwicklung von Gegenmaßnahmen gegen Cyberattacken wie sie in Situation (2) vermutet werden kann. Unser Fokus liegt hier wieder auf kritischen Infrastrukturen. Wir hoffen aber auch eine breitere Gruppe von Bedarfsträgern bedienen zu können, da potentielle neue Risiken aus der Verwendung der Cloud entstehen, die auch für anderen Nutzer von Bedeutung sind. Diese Risiken resultieren aus dem Cloud spezifischen Ansatz sich aus einem wide-area Netzwerk (oft das öffentliche Internet) mit (Cloud) Services zu verbinden und diese aktiv zu nutzen. Auch teilen sich Cloud-Systeme zu einem gewissen Grad Infrastruktur was z. B. Side Channel Attacken erlauben könnte. Die Cloud hat aber auch durchaus inhärente positive Attribute. Durch die dynamische Zurverfügungstellung von Ressourcen werden die Risiken einer Distributed Denial of Service (DDoS) Attacke zum Opfer zu fallen reduziert. Eine zusätzliche Herausforderung beim Verstehen, wie sich Risiken hier von traditionellen IT Systemen unterscheiden, ist die Abstraktion über Systemkomponenten. In SECCRIT werden daher etabliere Risikobewertungsmethoden auf System-immanente Probleme im Cloud- und kritische Infrastruktur-Bereich untersucht.

- Assurance Methoden beschäftigen sich mit dem Evaluieren bzw. Dokumentieren von Sicherheits-Features von Software bzw. Infrastrukturen. Dafür werden oft Zertifikate erstellt die dann laufend überprüft werden könne. Kritische Infrastrukturen stehen im Zentrum der öffentlichen Aufmerksamkeit, da Störungen weitreichende Folgen auf eine große Anzahl von „Nutzern" haben können. Es ist daher im Interesse der Betreiber und Nutzer, gewährleisten zu können, dass beim Erstellen z. B. der kritischen Infrastruktur Steuerungs-Software oder der kompletten Architektur auf bestimmte sicherheitsrelevante Aspekte (bzw. auch welche) getestet wurden. Im Rahmen von SECCRIT werden etablierte Methoden und Tools (wie z. B. Aspekte von Common Criteria) für den kritischen Infrastruktur & Cloud Bereich evaluiert.

Die weitere Liste an Anwendungsmöglichkeiten ist natürlich von den jeweiligen Use-Cases abhängig – grundsätzlich hoffen wir aus unserer Arbeit generelle Verbesserungen für Sicherheit „in der Cloud“ ableiten zu können, die sich auch auf Anwendungsfelder jenseits kritischer Infrastrukturen übertragen lassen.

4. Konklusion und zukünftige Arbeit

Wir haben in diesem Artikel gezeigt, welche sicherheitsrelevanten Themen im Bereich „Cloud Einsatz für kritische Infrastrukturen“ bzw. „Cloud als DIP-Technologie in der M2M Kommunikation“ unserer Forschungsarbeit bedürfen. Diese Themen wurden anhand eines Szenarios aus dem Projekt SECCRIT illustriert und deren Untersuchung motiviert. Weitere Szenarien werden in anderen Use Cases wie z. B. der „Cloudifizierung“ des Verkehrssteuerungssystems der Stadt Valencia untersucht. Die Untersuchungen sind im Rahmen der nächsten Jahre im SECCRIT Projekt geplant. Dies wird es ermöglichen, obige Themen bzw. die jeweiligen Lösungsansätze zu verifizieren und generischer zu gestalten. Wir hoffen dadurch in erster Linie aufzuzeigen ob und wie kritische Infrastrukturen Cloud Dienste nutzen können. Die Resultate werden neben Architekturvorschlägen, Methoden, Richtlinien auch Werkzeuge beinhalten, die einer breiten Gruppe von Bedarfsträgern zur Verfügung gestellt werden wird.

Danksagung

Das Projekt SECCRIT wird im Rahmen des EC FP7 Programms (Fördervertrag: 312758) gefördert.

Literatur

Peerenboom J., Fischer R., Whitfield R. (2001): Recovering from disruptions of interdependent critical infrastructures. In *Proc. CRIS/DRM/IIIT/NSF Workshop Mitigat. Vulnerab. Crit. Infrastruct. Catastr. Failures*.

Iankoulova I., Daneva M. (2012): Cloud computing security requirements: a systematic review. In *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on* (pp. 1-7). IEEE.

Cloud Security Alliance (2010): Top Threats to Cloud Computing V1.0. URL: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Burton S., Kaliski Jr., Wayne P. (2010): Toward risk assessment as a service in cloud environments. In *Proc. of the 2nd USENIX conference on Hot topics in cloud computing (pp. 13-13).* USENIX Association.

Dekker M. (2012): Critical Cloud Computing. ENISA .

Catteddu D., Hogben G. (2009): Cloud Computing Information Assurance Framework. ENISA.

Chandola V., Banerjee A., Kumar V. (2009): Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, 15.

Autoren

Markus Tauber
betreut AIT-Forschungsprojekte im Bereich Security in Cloud Computing, Kritische Infrastrukturen, Smart-Grids und Mobility. Dafür bringt er Erfahrungen aus seinen Projektleiter-Tätigkeiten bei dem ISP B.net – Teil des Multi-Utility-Providers BEWAG – und aus internationalen Forschungsprojekten an der „University of St. Andrews

(Scotland, UK)“ ein, wo er im Bereich „Networks and Distributed Systems” zum Thema „Distributed Storage Systems“ (Storage Clouds) promovierte und auch an anderen Themen arbeitet.

Christian Wagner

erlangte 2008 den Master of Science (MSc.) an der FH Technikum Wien, Österreich. Von August 2005 bis Mai 2009 war er als Software-Entwickler bei Philips Speech Recognition Systems GmbH mit der Entwicklung von Spracherkennungssystemen im medizinischen Bereich betraut. Seit Juni 2009 ist er am AIT Austrian Institute of Technology als wissenschaftlicher Mitarbeiter tätig, wobei sein Schwerpunkt in der Erforschung und Entwicklung sicherer Software-Infrastrukturen für kritische Infrastrukturen liegt.

Frank Pallas

studierte Informatik an der TU Berlin und promovierte dort im Jahr 2009. Seitdem ist er Mitarbeiter am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie (KIT) mit den Schwerpunkten Cloud Computing, Smart Grids und Elektromobilität. Zudem ist er seit 2011 Professor für Datenschutz und Informationsökonomik an der TU Berlin und seit 2013 auch am FZI Forschungszentrum Informatik im Bereich Cloud Computing tätig.