Sicheres IT-Auditing einer Cloud

Konzept zum sicheren IT-Auditing in unsicheren Umgebungen zur Erlangung von Vertrauen

Aljona Wehrhahn-Aklender und Norbert Pohlmann, Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen

Die Verbreitung der Cloud steigt. Mittlerweile nutzen über 60 % der deutschen Unternehmen Cloud-Dienste, zusätzlich planen knapp 20 %, zukünftig auf die Vorteile von Cloud-Lösungen zu setzen [1]. Mit der Cloud-Technologie sind jedoch auch vielfältige Herausforderungen hinsichtlich der IT-Sicherheit verbunden [2]. Aktuell wird die IT-Sicherheit einer Cloud primär durch den Cloud-Anbieter realisiert. Es gibt keine verlässliche Möglichkeit um zu kontrollieren, welche IT-Sicherheitsmechanismen dieser in der Cloud wie umsetzt. Im Besonderen diese Kontrollabgabe an einen externen Cloud-Anbieter verunsichert viele potenzielle Kunden [1]. Es stellt sich die berechtigte Frage, wie Unternehmen Vertrauen in die IT-Sicherheit von Cloud-Anbietern aufbauen können.

Secure Cloud Auditing

The popularity of the Cloud rises, but there is still much insecurity in the IT-Security of a cloud solution. Companies want to be able to check, if the processes in the cloud are secure and trustworthy. This is possible with an external auditing system, which compares measured data with predefined rules. But there is a chance, that the measured data are manipulated on its way to the auditing system, before leaving the cloud. To prevent these threads, the measured data must be protected right after it is generated. This is possible with the forward integrity method, which builds a chain-of-trust for the measured data without need of a TPM.

Keywords:
cloud, IT-Auditing, IT-Security

Gerade jene IT-Sicherheitsaspekte, die nicht ausgelagert werden können, weil sie eng an interne Prozesse gekoppelt sind, sind besonders relevant, wenn es um Vertrauenswürdigkeit geht und sollten von außen kontrolliert werden können. Bei solchen IT-Sicherheitsaspekten können unabhängige externe Auditoren die IT-Sicherheit der Cloud bestätigen [3]. Eine Remote Attestation nach dem Trusted Computing Standard ermöglicht ein automatisiertes Überprüfen und Attestieren von standardkonformen IT-Sicherheitsmechanismen [4], setzt aber voraus, dass jeder Rechner ein physisches Sicherheitsmodul, das TPM, integriert hat und in der Lage ist, dieses einheitlich anzuwenden. Die in diesem Beitrag vorgestellte IT-Sicherheitslösung benötigt kein TPM und kann folglich auch in heterogenen Infrastrukturen, wie sie üblicherweise bei einer Cloud vorliegen, verwendet werden.

In diesem Beitrag wird eine IT-Sicherheitslösung vorgestellt, die interne Cloud-Prozesse nach Vorbild des Trusted Computing Standards überwacht, ohne dass eine einheitliche TPM Abdeckung notwendig wird. Dies soll dazu beitragen, dass der Cloud-Anbieter die Abdeckung bestimmter IT-Sicherheitsstandards ohne einen Hardwareaustausch nachweisen kann und somit gewährleisten, dass IT-Sicherheitsstandards von Cloud-Anbietern eingehalten werden. Die IT-Sicherheitslösung soll das Vertrauen in Cloud-Anbieter deutlich steigern, da der Kunde einen ganzheitlichen Nachweis über die IT-Sicherheit der internen Cloud Prozesse erhält.

Externes IT-Auditing

Diese Kontrolle der internen Prozesse folgt dem Prinzip des externen IT-Auditing.

Unter dem Begriff IT-Auditing wird im Allgemeinen die Überprüfung von bestimmten Vorgaben innerhalb eines IT-Systems verstanden [5]. Hierbei steht in folgender Ausarbeitung eine Überprüfung der Cloud-internen Prozesse im Vordergrund. Das IT-Auditing dient zum einen der Protokollierung aller sicherheitsrelevanten Prozesse. Andererseits soll nachgehalten werden, ob die Prozesse den definierten Standardvorgaben und IT-Sicherheitsanforderungen genügen und erwartungsgemäß ablaufen [6]. Durch Automatismen soll das IT-Auditing auf Prozessebene kontinuierlich und parallel zur Laufzeit erfolgen.

Um ein sicheres und vollständiges IT-Auditing der Cloud-Prozesse zu ermöglichen, sollte das

Aljona Wehrhahn-Aklender studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

Prof. Dr. Norbert Pohlmann ist Professor für Informationssicherheit und Leiter des if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

pohlmann@internet-sicherheit.de
www.internet-sicherheit.de

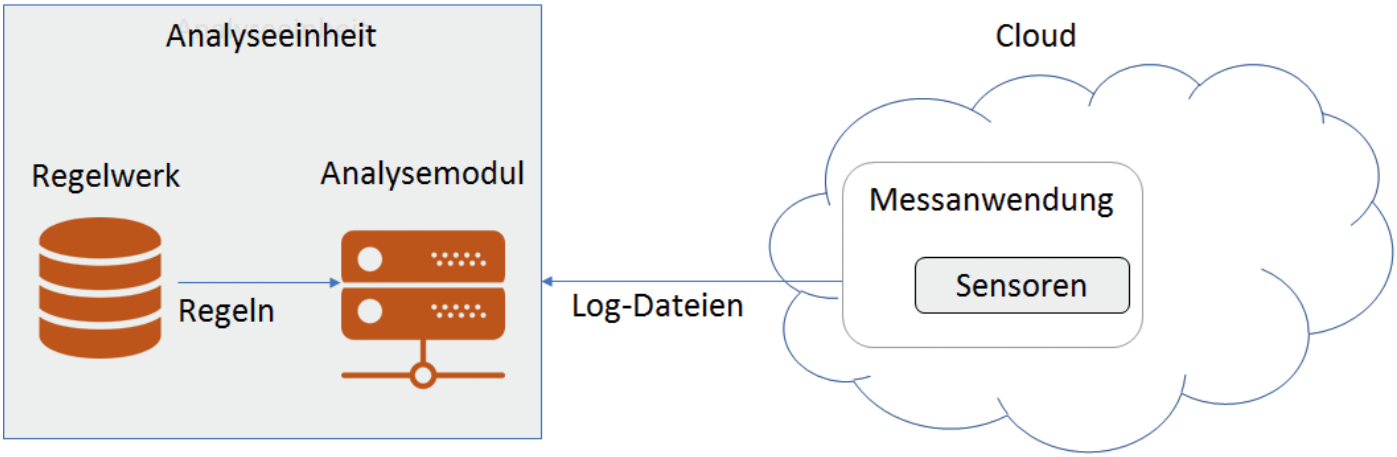

Bild 1: Automatisiertes, externes IT-Auditing.

IT-Auditing bestimmten IT-Sicherheitsvorgaben und standardisierten Anforderungen entsprechen. Diese Anforderungen können auf der ISO Norm 27001, den Anforderungen zum IT-Auditing des Cloud-Sicherheitsstandards CSA STAR und des IT-Grundschutzes aufbauen [6][7]. Durch sie lässt sich ein sicheres und standardisiertes Regelwerk aufbauen.

Das automatisierte, externe IT-Auditing setzt sich dafür aus mehreren Schritten zusammen. Zuerst werden der Prüfungsumfang und die Prüfungsinhalte festgelegt und als Referenzwerte und Richtlinien in einem Regelwerk definiert und gespeichert [5].

Daraufhin werden über definierte Messeinheiten, sogenannte Sensoren, die internen Prozesse innerhalb der Cloud-Infrastruktur gemessen. Die Rückmeldungen der Cloud zu ihren Operationen werden über diese Sensoren erfasst und von einer Messanwendung als Logs gespeichert. Die Messanwendung ist innerhalb der Cloud ein Cloud-eigener Dienst. Die gemessenen Daten werden zu einer externen Analyseeinheit übertragen und mit dem Regelwerk auf Konformität verglichen. Der Abgleich mit dem Regelwerk, sowie die Sicherstellung der Integrität und Vertraulichkeit der Daten sollte durch die externe Analyseeinheit gesteuert werden [8]. Diese Analyseeinheit vergleicht die gemessenen Werte und prüft auf Unregelmäßigkeiten oder Verstöße. Sie kann auch alarmieren, wenn Unregelmäßigkeiten oder Verstöße auffallen. Damit diese Analyseeinheit dem Anspruch auf Vertrauenswürdigkeit gerecht wird, sollte sie in der Kontrolle des Unternehmens verbleiben.

Bild 1 verdeutlicht das Prinzip des externen IT-Auditing. Hierbei generiert die Cloud bei jedem Prozess Werte, die von Sensoren erfasst und als Log-Dateien an die externe Analyseeinheit übertragen werden. Diese dient der Analyse der Log-Dateien und deren Vergleich mit den Regeln im Regelwerk.

Bei einem solchen IT-Auditing steht die IT-Sicherheit der Messdaten im Vordergrund. Die Log-Dateien werden von den Sensoren der Cloud erzeugt und müssen daraufhin die gesamte Cloud-Infrastruktur sowie das externe Netzwerk passieren, um die externe Analyseeinheit zu erreichen. Hierbei könnten sie von böswilligen Administratoren oder Angreifern aus dem externen Netzwerk eingesehen und verändert werden. Um dies zu verhindern, muss die Integrität und Vertraulichkeit der Log-Dateien sichergestellt werden. Diese Schutzziele sollten mit Blick auf die Vertrauenswürdigkeit nicht ausschließlich durch die Cloud, aber gleichzeitig möglichst früh Umsetzung finden, sodass Administratoren der Cloud sowie potenziell gefährliche Folgedienste keine Möglichkeit zur Einsicht oder Manipulation haben. Dabei ist zu klären, welche Aufgaben zum Schutz der Messdaten durch die externe Analyseeinheit abdeckbar sind und welche Aufgaben zwangsweise in der Cloud verbleiben müssen.

Die IT-Sicherheit von Log-Dateien

Sowohl die Vertraulichkeit als auch die Integrität von Log-Daten muss beim vorgestellten externen IT-Auditing geschützt werden. Dadurch, dass die Analyseeinheit eine externe Komponente ist, sind diese Schutzziele von besonderer Relevanz, da die Analyseeinheit keine direkte Messung vornehmen kann und auf Integrität und Vertraulichkeit der erhaltenen Werte vertrauen muss.

Um die Vertraulichkeit zu schützen, sollten Log-Dateien zwingend und schnellstmöglich verschlüsselt werden, damit sie über den gesamten Transferweg sicher vor Fremdeinsicht sind. Dies kann über symmetrische oder asym-

metrische Verfahren erfolgen. Der Vorteil bei asymmetrischen Verfahren ist hierbei, dass sie zusätzlich die Authentizität der Log-Daten schützen können. Die asymmetrische Verschlüsselung kann mithilfe eines Zertifikats erfolgen, in das ein öffentlicher Schlüssel (Public Key) eingebunden ist. Es bietet sich hierbei an, dass das asymmetrische Schlüsselpaar von der externen Analyseeinheit erzeugt wird und der private Schlüssel (Private Key) die externe Analyseeinheit zu keinem Zeitpunkt verlässt. Hierdurch wird sichergestellt, dass nur die externe Analyseeinheit die Log-Dateien wieder entschlüsseln kann, da nur sie den privaten Schlüssel zum Entschlüsseln besitzt. Außerdem kann die externe Analyseeinheit über die Verschlüsselung zusätzlich prüfen, ob die Log-Daten manipuliert wurden, da es die Log-Daten nur dann lesbar entschlüsseln kann, wenn sie nicht nachträglich verändert wurden (implizierte Integritätsprüfung). Der zusätzliche Gebrauch von sicheren Transferprotokollen wie HTTPS (TLS/SSL) trägt weiterhin dazu bei, dass eine sichere Kommunikation zwischen der Cloud und der externen Analyseeinheit gewährleistet ist. Unter Gebrauch der asymmetrischen Verschlüsselung lässt sich ein hohes Maß an IT-Sicherheit umsetzen. Es bietet aber auch Nachteile. Zum einen ist eine Ver- und Entschlüsselung mit einem asymmetrischen Verfahren aufwändiger als mit einem symmetrischen, zum anderen gibt es im vorgestellten Szenario nur ein Zertifikat mit einem Public Key. Dies bedeutet, dass die Verschlüsselung der Log-Daten potenziell von jeder Komponente der Cloud erfolgen könnte, die dieses Zertifikat besitzt. Es kann nicht überprüft werden, ob wirklich die Messanwendung die Log-Daten verschlüsselt hat oder ob dies zu einem späteren Zeitpunkt von jemand anderem, z. B. einem Angreifer, erfolgte. Es müsste für jede Messanwendung ein eigenes Publik-Key-Schlüsselpaar mit Zertifikat erzeugt werden. Dies würde den Ursprung der Log-Daten überprüfbar machen, ist zugleich aber mit hohem Aufwand hinsichtlich der Schlüssel und Zertifikatsgenerierung verbunden.

Wichtiger ist aber die Integrität der Log-Dateien. Denn nur wenn sicher ist, dass die Log-Daten nicht verfälscht sind, eignen sie sich zur Überprüfung der Standardkonformität und IT-Sicherheit der Cloud-Prozesse. Ein Verfahren, welches eine gute Möglichkeit zum Schutz der Integrität bietet, ist das Forward Integrity Verfahren. Bei diesem Verfahren wird ein neuer Log-Eintrag über ein Hash-Verfahren mit dem vorherigen Eintrag verkettet. Hierdurch wird der Schutz des neuen Eintrags über die Unverfälschtheit des vorherigen Eintrags sichergestellt und eine Vertrauenskette abgebildet (Chain-of-Trust). Sofern der erste Eintrag nicht manipuliert wurde, kann somit die Integrität aller Folgeeinträge über die Vertrauenskette realisiert werden [3]. Dieses Verfahren ähnelt dem Trusted Boot nach Trusted Computing Standard [4], benötigt jedoch kein TPM an der Messanwendung. Um das Vertrauen in den Ersteintrag sicherzustellen, sollte der erste Log-Eintrag, der sogenannte Root-of-Trust, von einem vertrauenswürdigen Erzeuger kommen. Im Falle der Ausarbeitung bietet sich die externe Analyseeinheit an. Diese kann ein TPM nutzen und dessen Root-Key über sichere Transferwege als Root-of-Trust für das Forward Integrity Verfahren übertragen.

Weiterhin sind an der externen Analyseeinheit zwei symmetrische Startschlüssel zu erzeugen. Mit diesen werden über ein Hash-Verfahren bei der Messanwendung zwei neue Schlüssel abgeleitet, die einerseits zur Verschlüsselung (Verschlüsselungsschlüssel), andererseits zur Erzeugung einer Prüfsumme (Integritätsschlüssel) genutzt werden. Durch weiteres Hashing der vorherigen Schlüssel werden immer weitere Schlüssel abgeleitet. Um die Vertrauenskette

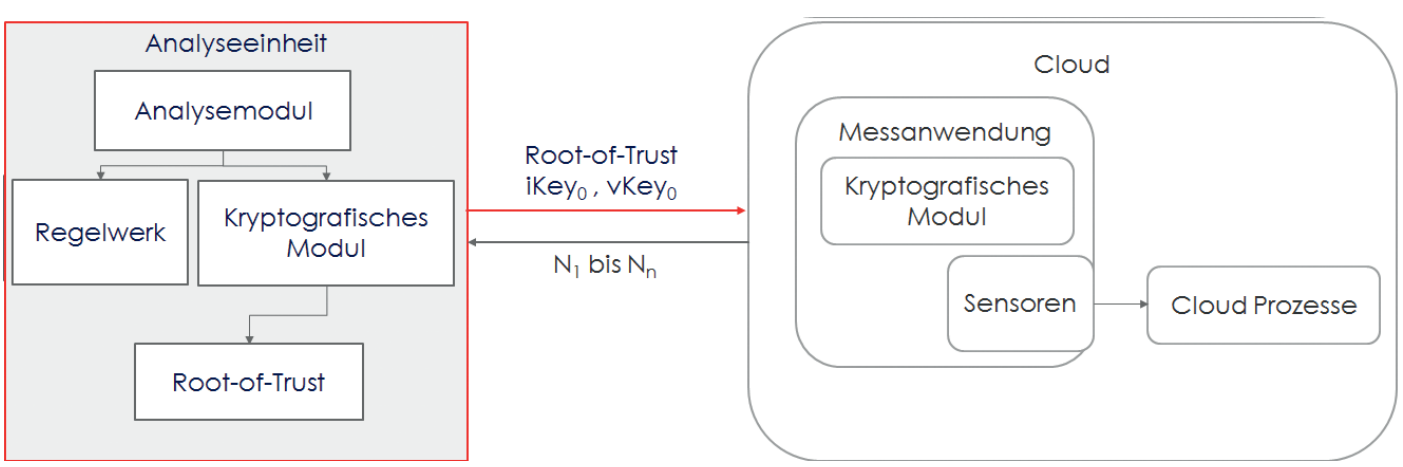

Bild 2: Übersicht des Forward Integrity Verfahrens mit externer Analyseeinheit.

aufzubauen, wird zuerst der erste Log-Eintrag mit Hinzunahme des Root-of-Trust und mit dem ersterzeugten Integritätsschlüssel zu einer Prüfsumme gehashed. In der Cloud wird danach ein Hashing jedes neuen Log-Eintrags mit der vorherigen Prüfsumme und mit dem jeweiligen neu erzeugten Integritätsschlüssel vorgenommen. Bei der Verschlüsselung der Log-Dateien wird auf den vom Startschlüssel abgeleiteten Verschlüsselungsschlüssel gesetzt.

Es ist wichtig, dass die Verknüpfung zur Chain-of-Trust schnellstmöglich innerhalb der Messanwendung geschieht, sodass die Log-Dateien die Cloud-Infrastruktur bereits integritätsgeschützt und verschlüsselt Richtung externe Analyseeinheit passieren können. Dadurch kann sichergestellt werden, dass kein Cloud-Dienst die Log-Dateien im Nachhinein beeinflussen kann. In dem Bild 2 werden die jeweiligen Komponenten des Forward Integrity Verfahrens mitsamt externer Analyseeinheit vorgestellt. Der Ablauf des Verfahrens ist wie folgt. Zuerst authentisieren sich Messanwendung und Analyseeinheit und bauen eine sichere Transferverbindung auf. Daraufhin werden von der Analyseeinheit zwei Startschlüssel (iKey0 und vKey0) erzeugt und mitsamt des Root-of-Trusts zur Messanwendung übertragen. Nun kann die sichere Transferverbindung geschlossen werden. Die Messanwendung leitet aus den Startschlüsseln Verschlüsselungsschlüssel und Integritätsschlüssel ab. Daraufhin beginnt die Messung. Der erste Logeintrag (L1) wird mit dem Root-of-Trust (R) unter Gebrauch des erstabgeleiteten Integritätsschlüssels (iKey1) zur Prüfsumme (P1) gehashed (P1= hashiKey1(R, L1)). Beide Daten werden vor einer Übertragung mit dem Verschlüsselungsschlüssel (vKey1) zu einem Nachweis (N1) verschlüsselt (N1= encvKey1(L1, P1)). Daraufhin werden die nächsten Schlüssel (iKeyn, vKeyn) abgeleitet und der nächste Logeintrag (Ln) mit der vorherigen Prüfsumme (Pn-1) gehashed (Pn= hashiKeyn(Pn-1, Ln)). Die Daten werden zur Analyseeinheit übertragen, welche entschlüsselt, die Chain-of-Trust verifiziert und danach die Log-Datei mit dem Regelwerk abdeckt.

Alle Startschlüssel sollten in der externen Analyseeinheit vorliegen, damit diese die abgeleiteten Schlüssel selber generieren kann [3]. Da alle Folgeschlüssel von den Startschlüsseln abgeleitet wurden, lassen sich die Folgeschlüssel zur Entschlüsselung und zur Überprüfung der Prüfsummen ableiten. Da die Root-of-Trust ebenfalls in der externen Analyseeinheit verwahrt ist, kann die externe Analyseeinheit die Integrität aller Log-Dateien durch die erzeugte Chain-of-Trust überprüfen, ohne dass es weitere Informationen von der Messanwendung benötigt. Es ist nötig, dass sich Messanwendung und Analyseeinheit auf einheitliche kryptografische Mechanismen zur Verschlüsselung und zum Hashing einigen.

Abschließende Beurteilung

Ein externes IT-Auditing bietet eine Möglichkeit, innere Cloud-Prozesse auf die Einhaltung bestimmter IT-Sicherheitsstandards zu überprüfen. Hierbei muss über IT-Sicherheitsmaßnahmen sichergestellt werden, dass die jeweiligen Prüfdaten nicht auf dem Weg zur Analyseeinheit verfälscht werden. Gerade in heterogenen Infrastrukturen, wie sie bei Cloud Lösungen zumeist vorliegen, kann hierfür nicht auf einheitliche Krypto-Module wie TPMs und folglich Maßnahmen wie einer Remote Attestation vertraut werden.

Das vorgestellte Forward Integrity Verfahren eignet sich gut zur Sicherstellung der Integrität und Vertraulichkeit in solchen Infrastrukturen, da es unabhängig von vorgegebener Hardware ist. Nachteilig ist aber, dass bei diesem Verfahren die Startschlüssel zur jeweiligen Messanwendung übertragen werden müssen. Dies muss geschützt erfolgen. An dieser Stelle sollte abgewogen werden, ob die Verschlüsselung der Startschlüssel nicht durch ein asymmetrisches Verfahren erfolgen sollte. Dies würde dazu führen, dass die Vertraulichkeit und Integrität der Schlüssel an ein asymmetrisches Verfahren abgegeben wird, während die Vertraulichkeit und Integrität der Log-Dateien über das Forward Integrity Verfahren Umsetzung finden. Jede Messanwendung müsste dafür ein eigenes Public-Key Paar generieren, damit nur es seine persönlichen Startschlüssel entschlüsseln kann. Eine Public-Key-Infrastruktur könnte notwendig werden.

Obwohl das Forward Integrity Verfahren eine gute Methodik zum Integritätsschutz und Vertraulichkeitsschutz von Prüfwerten in einer heterogenen Infrastruktur darstellt, schützt es nicht den Wahrheitsgehalt der Werte.

Inwieweit die gesammelten Messwerte richtig von den Sensoren erfasst und von der Messanwendung verarbeitet wurden, lässt sich nicht durch kryptografische Verfahren überprüfen. Hier muss ein Restvertrauen in die Cloud beziehungsweise in den Cloud-Anbieter bestehen.

Schlüsselwörter:
Cloud, IT-Auditing, IT-Sicherheit, Trusted Computing, Chain-of-Trust

Literatur

[1] Bitcom; Pols, A.; KPMG, Heidkamp, P.: Cloud Monitor – Eine Studie von Bitkom Research im Auftrag von KPMG. URL: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/Mai/Bitkom-KPMG-Charts-PK-Cloud-Monitor-12-05-2017.pdf, Abrufdatum: 26.11.2017
[2] Baun, C.; Kunze, M.; Nimis, J.; Tai, S.: Cloud Computing-Web-basierte dynamische IT-Services. Karlsruhe 2011.
[3] Kunz, T.; Niehues, P.; Waldmann U.: Technische Unterstützung von Audits bei Cloud-Betreibern. In: Datenschutz und Datensicherheit – DuD 37 (2013) 8, S. 521-525.
[4] Linnemann, M.; Pohlmann, N.: Turaya - Die offene Trusted Computing Sicherheitsplattform. In: Lutterbeck, B.; Bärwolff, M.; Gehring, R. (Hrsg): Open Source Jahrbuch 2007. Berlin 2007.
[5] Beißel, S.: IT-Audit. Grundlagen, Prüfungsprozess, Best Practice. Berlin 2015.
[6] Kersten, H.; Reuter, J.; Schröder, K.-W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung. Wiesbaden 2009.
[7] CSA Cloud Security Alliance, Cloud Control Matrix Working Group. URL: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview Abrufdatum: 26.11.2017
[8] Gräuler, M.; Martens, B.; Teuteberg, F.: Entwicklung und Implementierung einer Ontologie für das IT-Sicherheitsmanagement in Clouds. URL: http://www.user.tu-berlin.de/komm/CD/paper/ 061331.pdf, Abrufdatum 23.10.2016.