Bild: © Fotolia.com/belekekin

Cloud unter (eigener) Kontrolle: Trusted Cloud Enklave

Vertrauen durch Sicherheit

Die Cloud ist eine Top-Technologie, die mittlerweile sowohl in Unternehmen als auch bei Privatpersonen breit etabliert ist. Viele Branchenführer, wie zum Beispiel Amazon, IBM, Microsoft, Oracle und viele mehr, haben interessante Cloud-Lösungen entwickelt und bieten verschiedenste Services auf dieser Basis an. Aus Nutzersicht ergibt sich sehr oft ein Mix aus Services von verschiedenen Cloud-Providern, verbunden mit Zugriff auf Clouds verschiedener Hoster. Das macht die sichere Klärung der Frage, inwieweit die dabei anfallenden Daten vor Fremdeinsicht oder Manipulation geschützt sind, außerordentlich schwierig. Das Konzept der Trusted Cloud Enklave erlaubt Anwendern in diesem Szenario die durchgängige Kontrolle über ihre Daten.

Die Daten von Cloud-Nutzern werden durch die Services der Cloud Service Provider verarbeitet und durch einen Cloud-Hoster in einem externen Rechenzentrum verwaltet. Diese Parteien sind durch den direkten Kontakt mit Nutzerdaten folglich für die Umsetzung von IT-Sicherheit zuständig. Für einen Anwender bestehen kaum Möglichkeiten, diese Umsetzung nachzuvollziehen oder zu prüfen, ob die Maßnahmen standardisierten Sicherheitsansprüchen genügen. Dabei sind Nutzerdaten selbst dann verschiedensten Bedrohungen ausgesetzt, wenn die umgesetzten IT-Sicherheitsmaßnahmen vor Angriffen aus dem Internet oder vor anderen Anwendern schützen. Da der Cloud-Hoster physischen Zugang zur Hardware hat, kann er Zielsysteme physisch austauschen. Die Nähe zu den aktiven Systemen macht es auch möglich, Daten über die Abstrahlungen daraus aufzufangen.[1] Durch den direkten Zugriff kann der Hoster außerdem Klartextdaten direkt aus dem Speicher auslesen. Er kann sogar Schlüssel auslesen, sollte ein Verschlüsselungsverfahren diese in Klartext ablegen. Hierbei genügt es, wenn ein Master Key auf einem Speicher liegt, der für den Hoster physisch zugreifbar ist.

Der Cloud Provider kann hingegen über seine Services Zugang zu Klartextdaten erhalten. Das unterscheidet sich jeweils durch den verwendeten Dienst und ob dieser über eine Anwendung, über den Hypervisor oder direkt über den Zugang zur virtuellen Hardware Zugriff hat.[2] Durch geschickte Einbettung von Backdoors kann der Provider dabei sogar umgesetzte IT-Sicherheitsmaßnahmen umgehen. Folglich haben sowohl Hoster als auch Provider viele Möglichkeiten, an die Daten der Nutzer zu gelangen, ohne dass diese das mitbekommen würdene. Dem Nutzer fehlt es an Kontrollmöglichkeiten, um nötiges Vertrauen in Provider und Hoster zu entwickeln. Als Lösung des Problems bietet sich die Trusted Cloud Enklave an. Sie erlaubt eine sichere und vertrauenswürdige Nutzung von virtuellen Ar-

beitsplätzen und Anwendungen auf einer Cloud.[3]

Vertrauen durch Einbettung externer IT-Sicherheitssysteme

Die Trusted Cloud Enklave ist weitgehend unabhängig von der Cloud-Infrastruktur und folglich vom Hoster und Provider. Sie wird durch einen vertrauenswürdigen Drittanbieter gestellt und ist über Drittsysteme auf ihre IT-Sicherheitsabdeckung überprüfbar. Die Cloud-IT-Sicherheitslösung baut ein vertrauenswürdiges Netzwerk innerhalb der Cloud auf, das sich der direkten Kontrolle des Providers und des Hosters entzieht. Sie schützt die Authentizität und Integrität von Rechnern, die sich innerhalb einer Cloud befinden. Gleichzeitig schützt sie die Daten während des Transfers, im Speicher und während des Gebrauchs. Bei den Rechnern handelt es sich um IT-Systeme des Drittanbieters. Diese Rechner setzen messbare IT-Sicherheitsmaßnahmen um, die von externen Analysesystemen im Netzwerk der Nutzer ausgewertet werden können.

Die Vertrauenswürdigkeit wird dadurch gesteigert, dass alle IT-Sicherheitsmaßnahmen von außen überprüfbar sind. Die in der Cloud befindlichen Rechner bilden vertrauenswürdige (Trusted) Knoten. Sie setzen standardkonforme Sicherheitsmaßnahmen zum Eigenschutz, zur Stabilität und zur IT-Sicherheit von Daten um. Dabei vernetzen sie sich untereinander zu einem isolierten Bereich, indem der Datentransfer von der Restinfrastruktur entkoppelt ist. Dieser isolierte Bereich, zu dem nur die vertrauenswürdigen Knoten Zugang haben, beschreibt die Trusted Cloud Enklave (TCE).

Die Trusted Cloud Enklave wird als ein Netzwerk von vertrauenswürdiger Knoten definiert, die nicht über das Management der Cloud, sondern über ein Trusted-Cloud-Management verwaltet werden. Dieses befindet sich, wie auch bereits das externe Analysesystem, beim Nutzer. Das Analysesystem, das die Authentizität und Integrität von Trusted Knoten prüft, wird Security Gateway genannt. Das Security Gateway befindet sich innerhalb einer Client-/Server-Architektur zwischen den Thin-Clients des Anwenders sowie den Servern in der Cloud und dient als Zugangspunkt zum Rechenzentrum. Eine Besonderheit eines Security Gateways ist, dass die Anzahl an unterstützten Endknoten variabel sein kann, sowohl hinsichtlich der Client- als auch der Server-Endgeräte. Dies bedeutet auch, dass verschiedene interne Netzwerke über das Security Gateway auf verschiedene Clouds zugreifen können. Die Server-Endgeräte sind im konkreten Fall verteilt auf mehrere Clouds, während die Clients im verteilten Nutzernetz eingebunden sind (siehe Abbildung 1). Durch die damit gegebene Flexibilität kann die Lösung cloud-unabhängig umgesetzt werden. Die Trusted Cloud Enklave wird von außen durch das Security Gateway administriert, überwacht und überprüft.

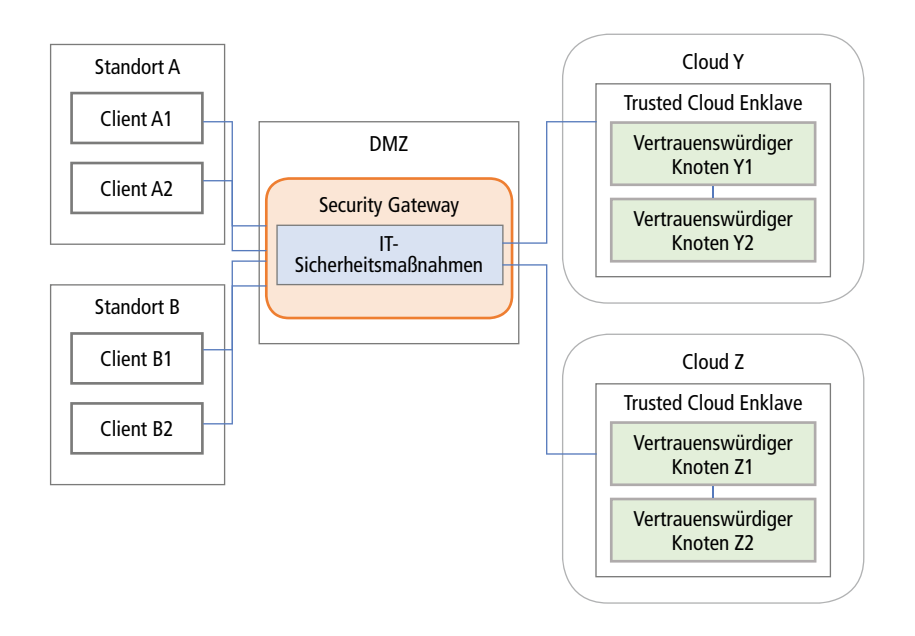

Abbildung 1: Übersicht Trusted Cloud Enklave

Zusammensetzung einer Trusted Cloud Enklave

Um Cloud Services nutzen zu können, müssen die Knoten in der Cloud von den Services der Provider angesprochen werden können. Die Trusted Knoten einer Trusted Cloud Enklave bauen deswegen funktional auf der Infrastruktur der Cloud auf, aber erweitern sie um eigene Funktionalität und IT-Sicherheitsmaßnahmen zum Schutz von Vertraulichkeit und Integrität. Das erlaubt, dass diese integrierten Knoten die Vorteile einer vorhandenen Cloud-Infrastruktur nutzen, aber ihre IT-Sicherheit unabhängig vom Provider und nicht manipulierbar für den Hoster bleibt. Hierbei besteht ein Trusted Knoten aus verschiedenen Hardware- und Softwarekomponenten.[3]

Um der Bedrohung durch physische Angriffe oder durch Angriffe auf Hardwareprozesse entgegenzuwirken, bauen die Knoten auf sicherer, vertrauenswürdiger Hardware, sogenannter Trusted Hardware, auf. Die Trusted Hardware setzt sich aus gehärteten Hardwaresicherheitsmodulen zusammen, die vor physischen Angriffen sowie vor gezielten Angriffen auf ihre Prozesse geschützt sind. Zu den Hardwaresicherheitsmodulen zählt unter anderem ein Trusted Platform Module (TPM). Dieses ist ein physisch isoliertes Sicherheitsmodul, durch das die Integrität eines IT-Systems durch Verfahren wie den Trusted Boot geschützt ist.[4]

Die Hardware wird je nach Anwendungszweck mit verschiedener, vertrauenswürdiger Software bespielt. Dies erfolgt durch das minimale, sichere Betriebssystem (Trusted OS, beziehungsweise Trusted Firmware), das

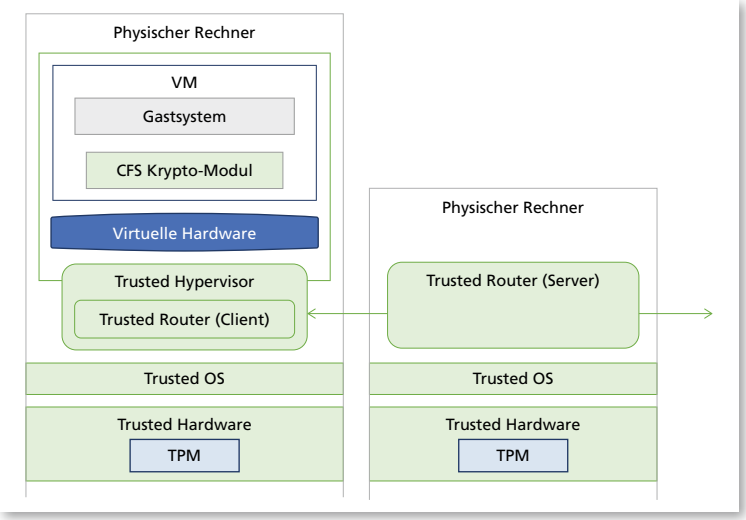

Abbildung 2: Trusted Knoten mit Trusted Hypervisor (links), Trusted Knoten mit Trusted Routing Server (rechts)

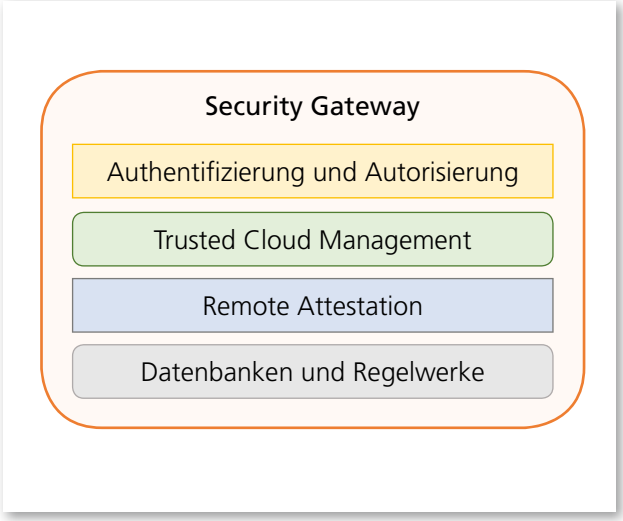

Abbildung 3: Funktionen eines Security Gateways

sich bereits initial auf der Hardware befindet. Hierfür – ebenso für weitere IT-Sicherheitsmaßnahmen – interagiert das Trusted OS mit dem TPM der Trusted Hardware. Bei der vertrauenswürdigen Software, die installiert wird, kann es sich um eine von zwei Varianten handeln. Wenn der Knoten als eine vertrauenswürdige Ausführungsplattform für Gastsysteme konzipiert ist und folglich dem Anwender sichere, virtuelle Arbeitsplätze zur Verfügung stellen soll, wird der Trusted Hypervisor aufgespielt. Dieser übernimmt die sichere Einbettung und Verwaltung der Arbeitsplatz-Gastbetriebssysteme oder Arbeitsplatz-Anwendungen und setzt dafür unter anderem starke Separierungs- und Isolierungsmechanismen für die virtuellen Ressourcen um. Der Trusted Hypervisor ist zusätzlich mit einem CFS-Krypto-Modul ausgestattet (Crypto-File-System), welches für die Verschlüsselung von Nutzdaten vor der Speicherung zuständig ist. Für die Wegeverschlüsselung wird außerdem der Baustein Trusted Routing Client eingebunden (siehe Abbildung 2, links). Dient der Knoten hingegen der sicheren Vernetzung der virtuellen Arbeitsplätze, wird der Trusted Router in der Ausprägung Trusted Routing Server aufgespielt. Dieser übernimmt die Funktionen eines sicheren Switches und Routers. Der Trusted Routing Server schützt dabei den Datenverkehr zum Security Gateway und baut sichere Netzwerke zwischen den vertrauenswürdigen Knoten der Cloud auf (siehe Abbildung 2, rechts).

Die Integrität der vertrauenswürdigen Knoten ist durch Verfahren wie dem Trusted Boot der Trusted Computing Group geschützt. Dies stellt sicher, dass Manipulationen an der Trusted Cloud Enklave schwer realisierbar sind. Die innerhalb der Trusted Cloud Enklave transportierten Daten können ausschließlich über den Trusted Routing Client transportiert werden. Hierbei erfolgt eine Zwangsverschlüsselung, die sicherstellt, dass die Daten nur bei anderen vertrauenswürdigen Knoten oder im Nutzernetz entschlüsselt werden können. Durch diese abgrenzende Verschlüsselung von Daten im Transfer und Speicher können diese nicht außerhalb der Trusted Cloud Enklave oder des Nutzernetzes eingesehen werden. Eine Trusted Cloud Enklave besteht zusätzlich zu den Trusted Knoten auch aus den vom CFS-Krypto-Modul verschlüsselten Speicherbereichen der Speichermedien. Der Verbund kann über das Security Gateway beliebig um neue Trusted Knoten und Speichermedien erweitert werden. Zusätzlich übernimmt das Security Gateway eine Vielzahl weiterer bedeutender Funktionen (siehe auch Abbildung 3).

Kontrollübergabe durch den Nutzer

Die Trusted Knoten in der Cloud dienen dazu, eine Trusted Cloud Enklave aufzubauen, welche die sichere Nutzung von Gastsystemen sowie von virtuellen Arbeitsplätzen ermöglicht. Sie bilden die vertrauenswürdige Ausführungsumgebung für diese Gastsysteme. Sie können ihre Schutzfunktion aber nur dann ausüben, wenn sie auch tatsächlich in die Cloud-Infrastruktur eingebunden wurden und dabei keine Manipulation am Knoten erfolgte. Diese Anforderungen lassen sich durch das Security Gateway überprüfen. Anders als die vertrauenswürdigen Knoten in der Cloud, befindet sich das Security Gateway außerhalb der Cloud-Infrastruktur und ist dadurch geeignet, um wichtige Kontrollfunktionen zu übernehmen. Es schützt die Trusted Cloud Enklave vor Angriffen auf ihre Integrität und vor unerlaubtem Zugriff.

Um die Authentizität und Integrität der Trusted Knoten zu schützen, dient das Security Gateway als Verifier (Prüfstelle) bei einer „Remote Attestation" nach Trusted Computing Group. Eine Remote Attestation ist als das Reporting eines Systemstatus an ein externes Überprüfungsmodul definiert, welches Rückmeldung über die Integrität des IT-Systems und dessen Bestandteile geben kann. Dies ermöglicht die Authentifikation des IT-Systems und sichert gleichzeitig, dass dieses IT-System nicht manipuliert ist.[5] Der Systemstatus wird üblicherweise über das Platform Configuration Register (PCR) in einem TPM abgebildet.[4]

Im Security Gateway befindet sich auch noch das Trusted Cloud Management, wel-

ches die Verwaltung einer Trusted Cloud Enklave übernimmt und damit die Verwaltung in das Nutzernetz verschiebt. Somit entzieht sich die Trusted Cloud Enklave der Administration eines Cloud-Hosters. Als zentraler Zugangspunkt zur Cloud überprüft das Security Gateway zusätzlich sowohl die Authentizität der Anwender, als auch die Authentizität der Server in der Cloud. Es übernimmt neben der Authentisierung auch die Autorisierung der anfragenden Anwender und leitet Anfragen zur Anmeldung passend an die Clouds weiter. Da das Security Gateway verschiedene Endknoten unterstützt, lassen sich hierüber auch verschiedene Cloud-Anbieter einbinden.

Des Weiteren beinhaltet das Security Gateway alle sicherheitsrelevanten Regelwerke und Datenbanken, die für eine Überprüfung notwendig sind. Dadurch können Regelwerke und Datenbanken je nach den Ansprüchen des Anwenders durch definierte Policies und Properties jederzeit angepasst werden. Sie befinden sich unter der Kontrolle des Anwenders und lassen sich folglich nicht unbemerkt verändern. Durch die Auslagerung dieser IT-Sicherheitsmaßnahmen (zusammenfassend in Abbildung 3 dargestellt) in ein zentrales Gateway im Nutzernetz ist dieses als Managementsystem für die Trusted Cloud Enklave sehr gut für einen Administrator aus dem Nutzernetz heraus ansprechbar. Das Security Gateway kann alternativ auch von einem vertrauenswürdigen Drittanbieter betrieben werden.

Zusammenfassung und Abgrenzung der Lösung

Parallel mit dem wachsenden Interesse an Cloud-Lösungen steigt der Bedarf nach Vertrauenswürdigkeit in der Cloud. Dieser Bedarf kann nicht nur durch Aussagen des Cloud-Hosters oder des Cloud Providers zu deren IT-Sicherheitsmaßnahmen gedeckt werden. Aus diesem Grund wird eine Cloud-IT-Sicherheitslösung benötigt, die unabhängig von den IT-Sicherheitsmechanismen der Provider und Hoster ist. Mit der Trusted Cloud Enklave wurde eine möglichst unabhängige Lösung konzipiert, durch die virtuelle Arbeitsplätze sicher in einer Cloud genutzt werden können. Diese Arbeitsplätze werden dazu in vertrauenswürdige Knoten einer Trusted Cloud Enklave eingebunden. Unter Zuhilfenahme eines Security Gateways lassen sich diese Trusted Knoten als sichere Ausführungsumgebungen für Gastsysteme nachweisen. Dabei setzt sich eine Trusted Cloud Enklave aus Trusted Hardware mit Trusted Firmware zusammen, auf die entweder ein Trusted Hypervisor oder

ein Trusted Router installiert wird. Die Trusted Knoten in der Cloud werden über eine Remote Attestation bei Erstinstallation sowie bei jedem Systemstart und bei Bedarf auf ihre Integrität und Standardkonformität überprüft. Die Sicherheitsfunktionen der verschiedenen Trusted Komponenten decken die Bedrohungen für eine Cloud hinsichtlich Integrität, Datensicherheit und Angriffsschutz ab, so dass eine Trusted Cloud Enklave eine geschützte Ausführungsumgebung für virtuelle Arbeitsplätze abbildet. Ein Anwender weiß, dass seine Daten sicher übertragen, verarbeitet und verschlüsselt gespeichert werden.

Durch die Trusted Cloud Enklave werden die meisten Sicherheitsanforderungen zur Verwendung von Gastsystemen auf der Cloud umgesetzt, nur wenige Anforderungen an Hoster und Provider bleiben bestehen. Diese betreffen beispielsweise die Verfügbarkeit. Der Cloud Hoster ist dafür zuständig, dass Rechenzentren redundant vernetzt und vor Umwelteinflüssen gesichert sind. Dagegen liegt es in der Verpflichtung des Cloud Providers, seine grundlegenden Prozesse auf aktuellen IT-Sicherheitsstandards zu halten und die Verfügbarkeit technisch zu gewährleisten. Neben diesen Restanforderungen bietet die Trusted Cloud Enklave mit Security Gateway einen umfangreichen Schutz, der alle zuvor genannten und darüber hinaus noch einige weitere Angriffsszenarien abdeckt. Um eine Trusted Cloud Enklave umzusetzen, wird eine Cloud Infrastruktur benötigt, die das Einbetten der Trusted Komponenten unterstützt und dessen Services durch die Trusted Komponenten gesteuert werden können. Eine solche Cloud-Lösung stellt beispielsweise OpenStack dar, bei der sich die Cloud Infrastruktur aus quelloffenen, atomaren und anpassbaren Servicegruppen zusammensetzt.[6]

Die hohe IT-Sicherheitsabdeckung der Lösung bringt auch Einschränkungen bei den Services mit sich: Da der Zugriff des Providers durch die Lösung limitiert ist, lassen sich etwa Services einer Cloud, die auf dem freien Zugriff auf virtuelle Ressourcen aufbauen, nicht mehr nutzen. Auch die üblichen Verfahren einer Cloud zur Leistungssteigerung wie die Migration von VMs, können nach aktuellem Stand der Dinge nicht mehr verwendet werden. Die meisten Cloud-Infrastrukturen setzen diese dynamische Migration ganz selbstverständlich um, um virtuelle Ressourcen optimal auf physische Ressourcen zu verteilen.[7] Eine Migration von VMs auf einer Trusted Hardware führt aber zum Datenverlust, da die Daten im CFS an die Hardware gebunden sind und nur dort entschlüsselt werden können. Das ist der Preis dafür, dass die Verfahren zur Datensicherheit nicht durch eine Migration auf eine potenziell unsichere Plattform ausgehebelt werden können.

Um die Migration von VMs bei Einhaltung der IT-Sicherheit zu ermöglichen, müssten Schlüsselwerte nicht zwingend an das TPM der Trusted Hardware gebunden sein, sondern ebenfalls flexibel auf andere Trusted Hardware einer Trusted Cloud Enklave migriert werden können. Für diese Anforderung kann eine Managementkomponente entwickelt werden, die einen zentralen Schlüsselspeicher abbildet und die Migration von Schlüsseln und virtuellen TPMs (vTPMs) verwaltet. Eine solche Lösung könnte in das Security Gateway eingebunden werden. Diese Entwicklung ist jedoch getrennt vom vorgestellten Konzept zu betrachten. Das beschriebene Konzept ermöglicht unabhängig von der Migration ein sicheres Arbeiten auf Rechnern in der Cloud. Sie räumt also Bedenken hinsichtlich der Vertrauenswürdigkeit der Cloud-Infrastruktur aus dem Weg, da die gehärteten Knoten aus dem Nutzernetz heraus auf ihre IT-Sicherheit überprüft werden können. ■

ALJONA WEHRHAHN-AKLENDER
studierte im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigte sich im Rahmen des Studiums mit der Sicherheit von und dem Vertrauen in Cloud-Lösungen.

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Referenzen:

[1] *Ravi, S., Raaghunathan, A., & Chakradhar, S. (2004). tamper Resistent Mechanisms for Secure Embedded Systems. 17th International Conference on VLSI Design.*

[2] *Bothe. (2015). Datenschutz und Datensicherheit im Cloud Computing. Von www.unibremen.de: http://eddi.informatik.unibremen.de/ SUSE/pdfs/Diplomarbeit_Steffen_Bothe.pdf am 22.03.2018 abgerufen*

[3] *Wehrhahn-Aklender, A. (2018). Trusted Cloud Enklave – Konzepte zum Schutz virtueller Arbeitsplätze in unsicheren Cloud Infrastrukturen*

[4] *Chen, L., Mitchell, C., & Martin, A. (2009). Trusted Computing – Second International Conference. Berlin: Springer.*

[5] *Pohlmann, N., & Reimer, H. (2008). Trusted Computing – Der Weg zu neuen IT-Sicherheitsarchitekturen. Wiesbaden: Friedr. Vieweg & Sohn Verlag.*

[6] *Beitter, T., Kärgel, T., Zielenski, S., Steil, A., & Nähring, A. (2014). IaaS mit OpenStack: Cloud Computing in der Praxis. Heidelberg: dpunkt Verlag.*

[7] *Frey, S., & Hasselbring, W. (2011). The CloudMIG Approach: Model-Based Migration of Software Systems to Cloud-Optimized Applications. Von www. geomar.de: http://oceanrep.geomar.de/14431/1/soft_v4_n34_2011_8.pdf am 21.01.2018 am 22.03.2018 abgerufen*