:get know howww
UBIT Steiermark

Bildungsthema

CLOUD STRATEGIE – SIND SIE SCHON DRIN?
Einstieg – Umstieg – Ausstieg mit der Cloud

Themenexperten:

IT Security ExpertsGroup der WKÖ – www.itsecurityexperts.at

DI Gerald Kortschak, CMC,
Sprecher Arbeitskreis IT Security Experts Steiermark

Harald Wenisch,
Wenisch Consulting e.U.

Co-Autoren dieses Kapitels:

IT Security ExpertsGroup WKÖ – Inhalte des Cloud-Strategy-Papers

HansChristian Einfalt - sevian7 IT development GmbH

Florian Brunner, BSc - Holistic Security Consulting GmbH

Christian Gegenhuber, edv.service.gegenhuber OG

Erik Rusek, BSc – Holistic Security Consulting GmbH

Siegfried Schauer – IKARUS Security Software GmbH

DI Martin Schober – MSC martin.schober

März 2014

Inhaltsverzeichnis

1 KAPITEL 3 – Ausstieg aus der Cloud

Einleitung

Der Ausstieg aus der Cloud muss mindestens ebenso gut geplant werden wie der Einstieg - und zwar möglichst bereits zum selben Zeitpunkt. Konkret sollte mit Anbietern/Implementierern/Projektverantwortlichen bereits zu Beginn des Projektes ein Ausstiegsszenario erstellt werden. Die Bereitschaft, ein solches bereitzustellen bzw. Strategien und Szenarien für einen Austieg/Anbieter- Wechsel parat zu haben, ist mit ein Qualitätsmerkmal eines guten Anbieters. Gründe für den Aus- oder Umstieg gibt es viele, sie sind ebenso zahlreich wie die Gründe für einen Einstieg. Tatsächlich kann (fast) jedes Einstiegs- auch als Ausstiegsargument verwendet werden. Angefangen bei einfachen Gründen wie Plattform- oder Anbieter-Wechsel, über eine geänderte Finanz-/Status-/Firmenlage bis hin zu Sicherheits- und/oder Compliance-Thematiken lassen sich zahlreiche mögliche Szenarien finden.

Grundsätzliche Erwägungen basieren letztendlich auch auf der Art der Cloud-Nutzung. Bei einer Storage-Lösung ist der Aus- respektive Umstieg voraussichtlich leichter zu bewerkstelligen als bei SaaS-, IaaS- oder PaaS-Ansätzen.

Der Schwierigkeitsgrad lässt sich den Ansätzen aufsteigend zuordnen:

SaaS – PaaS – IaaS Während bei IaaS (Infrastructure as a Service) eine komplette Landschaft (neu) erschaffen werden muss, beschränkt sich der Aufwand bei SaaS auf das Migrieren von Datenbeständen und Prozeduren.

Dies, das Migrieren von Datenbeständen und Prozeduren, ist zwar grundsätzlich nicht einfach, lässt sich aber im Allgemeinen mit Hilfe der (notwendigerweise bereits vorhandenen) Prozessbeschreibungen und Firmenrichtlinien mehr oder weniger linear abbilden.

Der Ausstieg

Der komplette Ausstieg aus der Cloud

Ein Ausstieg aus der Cloud kann ein kostspieliges Unterfangen werden.

War der Einstieg in die Cloud von Zielen der Kostenersparnis getrieben, so muss der Ausstieg einer mittel- bis langfristigen Kalkulation unterzogen werden, da einige Kostenfaktoren, die beim Einstieg weggefallen waren, (wieder) zu berücksichtigen sind.

Abhängig vom jeweiligen Modell der Cloud-Nutzung sind folgende Faktoren zu betrachten:

– Infrastruktur

Wird die Infrastruktur, die zum Zeitpunkt des Ausstieges in der Cloud existiert (IaaS) zurückgeholt, muss eine entsprechende lokale Struktur geschaffen werden. Dies reicht vom breitbandigen, ausfallsicheren und hochverfügbaren Internet-Zugang über Firewall und IDS bis hin zu Racks und Serverraum inkl. Wartung und Kühlung.

– Mitarbeiter

Die neu zu schaffende Infrastruktur muss betreut und gewartet werden, sei es durch externe Dienstleister oder eigene Mitarbeiter.

– Arbeitsplätze

Liegt der Arbeitsplatz des Mitarbeiters nicht mehr in der Cloud, wie dies bei Teleworkern oft der Fall ist, sondern zukünftig lokal, muss entweder ein entsprechender hochverfügbarer Zugang (inkl. entsprechender Inhaltsanpassungen in Arbeits-Verträgen) oder ein entsprechender Arbeitsplatz inkl. Schreibtisch, Bestuhlung und Beleuchtung geschaffen werden. Weiters muss ein dem Gesetz entsprechendes Arbeitsumfeld (Sanitär- und Rekreationseinrichtungen, Anfahrtsmöglichkeiten, etc.) vorhanden sein.

– Backup

Liegen die Daten nicht mehr „in der Cloud“ muss spätestens zu diesem Zeitpunkt ein entsprechendes Backup-Konzept umgesetzt werden, das nicht nur den gesetzlichen Vorgaben genügt, sondern auch alle in den Firmenvorgaben festgelegten Szenarios betrachtet (und vielleicht ein oder zwei, die bei der Entwicklung der Firmenvorgaben unbeachtet blieben).

– Lizenzen

Vom Cloud-Provider bereitgestellte Lizenzen werden voraussichtlich nicht mehr zur Verfügung stehen und müssen durch eigene ersetzt werden.

– Sicherheitsaspekte

Sicherheitsmechanismen und -funktionen, die in der Cloud seitens des Providers bereitgestellt werden (müssen), sind im Szenario „on premise“ selbst bereit zu stellen, zu warten und aktuell zu halten. Eine regelmäßige Überprüfung der Sicherheitseinrichtungen ist ebenso einzuplanen und durchzuführen.

– Qualitätskriterien, Qualitätssicherung, Qualitätsmanagement

In der eigenen Cloud, im eigenen Datacenter etc, sind die gleichen Qualitätskriterien anzuwenden, wie sie für den Cloud-Anbieter vor dem Ausstieg gegolten hatten. Dies betrifft alle Aspekte des Services von der Verfügbarkeit bis hin zur Verschlüsselung. Qualitätssicherungsmechanismen und -funktionen, die in der Cloud seitens des Providers bereitgestellt werden (müssen) sind im Szenario „on premise“ selbst zu definieren, bereit zu stellen und umzusetzen. Audits und Reviews sind nicht nur im Bereich Sicherheit sondern auch im Qualitätsmanagement mindestens im gleichen Umfang durchzuführen wie zuvor vom Provider zur Verfügung gestellt bzw. im SLA festgehalten.

Zu klären sind weiters folgende Punkte:

– wer bewahrt die Daten aus bzw. in der Cloud auf? Ist dies der Provider (unwahrscheinlich ohne Vertrag und Abgeltung) oder der (Ex-) Kunde?

Im Allgemeinen wird die Verantwortung auf den Kunden übergehen, der nun dafür zu sorgen hat, dass den entsprechenden Vorschriften Genüge getan wird.

– Gleiches gilt sinngemäß für Backups und Signatur- oder Verschlüsselungs-Keys, die über die gesamte Dauer der Verwendung und Lagerung vorgehalten werden müssen.

– Das Vorhalten der Daten, sowie deren (vollständige) Löschung nach dem Ausstieg müssen mit angemessenen Übergangsfristen und realistischen Zeiträumen versehen werden. Weder wird der Provider die Datenbestände ewig vorhalten wollen, noch wird von ihm, ohne entsprechende vertragliche Vereinbarung, eine vollständige Löschung durchgeführt werden, denn beides kostet Geld.

– Zu betrachten ist bei der Planung eines Ausstieges ebenso, wie eine Rückforderung der Daten, Backups und Keys erfolgen kann/soll/muss.

Oft sind die eingesetzten Lösungen nicht offen, sondern an bestimmte Infrastruktur-Produkte gekoppelt, ein Ausstieg (oder auch nur Umstieg) ist in diesem Fall nur einfach möglich, wenn die entsprechenden Systeme weiter eingesetzt werden. Dies betrifft in erster Linie die eingesetzte Software, da hier oft Inkompatibilitäten existieren, die den Umstieg erschweren und kostspieliger machen. Man spricht hier auch vom Vendor Lock In, also der Abhängigkeit von einem Hersteller. Ist dies der Fall kann man entweder dem Diktat folgen, die Software weiter lizensieren und damit im Joch verbleiben, oder den Rat und die Unterstützung von Experten einholen, um die in Frage kommenden Daten zu entkoppeln. Dies ist zwar meist mit Aufwand (zeitlich und finanziell) verbunden, auf lange Sicht aber der weitaus günstigere Weg, da danach einer Migration selten große Hürden entgegenstehen.

Umstieg, Provider-Wechsel, Wechsel von public zu private cloud

Bei einem Umstieg, also dem Wechsel von einem Provider zu einem anderen, hängt das anzuwendende Szenario vorrangig davon ab, ob mit dem Provider- auch ein Struktur-Wechsel verbunden ist.

Wird die Plattform (z.B. bei Virtualisierungen) beibehalten, so kann es ausreichen, die (virtuellen) Ressourcen aus Backups auf der neuen Infrastruktur (bei dem neuen Provider oder im eigenen Datacenter) wiederherzustellen. Denkbar ist ebenso eine Live-Migration aus der alten in die neue Infrastruktur, wie sie z.B. Citrix/XEN, VMWare oder Hyper-V mit ihren Virtualisierungsservern bieten.

Ein anderer Ansatz, allerdings ungleich aufwändiger, ist die komplette Neuerstellung der Installationen. Dies ist meist dann der einzige Ausweg, wenn der alte Provider (berechtigt oder unberechtigt) die bis dato genutzten Ressourcen nicht zur Übertragung freigibt. Oft werden dabei lizenztechnische oder -rechtliche Gründe ins Treffen geführt die aber, bis auf wenige Ausnahmen, meist vorgeschoben sind. Eine Abklärung im Vorfeld des Vertragsabschlusses ist hier jedenfalls anzuraten.

Bei einem Plattform-Wechsel, z.B. von einem System-Anbieter zum anderen, bieten die jeweiligen Plattform-Hersteller Tools zur Migration an, deren Einsatz allerdings ebenfalls vom Willen des und der Unterstützung durch den alten Provider abhängig ist.

Hier kann die Neuerstellung der Ressourcen ebenfalls das kleinere der beiden Übel sein.

Im Falle von Storage-Cloud-Lösungen gestaltet sich die Migration üblicherweise einfacher, da „lediglich“ Daten verschoben werden müssen. Ein Verbinden der diversen Dienste stellt hier die einfachste Lösung dar.

Ein weiterer Ansatz, besonders im Falle verschlüsselter Datenspeicher, kann sein Backups aus lokalen Repositories wiederherzustellen. Bei verschlüsselten Speichern empfiehlt es sich auch, die entsprechenden Schlüssel (Ringe) nach Beendigung der Migration zu deaktivieren bzw. zu revokieren. Bei sensiblen Datenbeständen, besonders im Gesundheitsbereich, ist ebenso eine entsprechende Erklärung des Storage-Providers über die Sicherheit und Qualität der Verschlüsselung zu empfehlen, ebenso muss, im Fall der Übergabe von Daten (Produktiv- und Sicherungsdaten, etc.), ein entsprechendes Protokoll über die sichere Vernichtung vom alten Provider verlangt werden.

Als eine Sonderform des Ausstieges resp. der Hybrid-Cloud kann ein dynamisches Nutzen der Cloud angesehen werden, d.h. das Nutzen von Cloud-Ressourcen für eine kurze Zeit (Stunden), um etwa Lastspitzen abzufangen oder Test- und Entwicklungsumgebungen kurzfristig bereit zu stellen. Dies ist die wohl innovativste Form der Cloud-Nutzung und bietet dem Anwender viele Vorteile.

Die Aufgabenstellungen sind hier nicht nur im Bereich der technischen Umsetzung, sondern und vor allem in der Abrechnung zu sehen. Die meisten Anbieter bieten Abrechnungsmodelle an, die über Laufzeiten und Volumina definiert sind (Monats- oder Jahresverträge, Bandbreiten-, Transfer- oder Transaktions-Volumen). Eine Abrechnung nach echter Nutzung ist aufwändig, bringt zwar dem Kunden wahrscheinlich Vorteile, nicht aber dem Anbieter. Die Chancen einen Vertag mit echter Pay-per-Use Abrechnung zu finden sind also aus aktueller Sicht eher gering.

Technische Lösungen und externe Unterstützung

Die technische Auflösung des Problems Um-/Ausstieg hängt in erster Linie von der Ausgangssituation ab (SaaS/PaaS/IaaS, Storage, Virtualisierung).

In vielen Fällen wird der technische Support des neuen Anbieters/Providers Unterstützung anbieten können, darüber hinaus lassen sich einige Spezialisten unter den IT-Dienstleistern finden.

Es empfiehlt sich, den Um- bzw. Ausstieg ausreichend zu planen und Spezialisten in das Projekt zu holen. Ausreichend Zeit, gute Planung und ein Budget, das den Namen verdient, sind die besten Voraussetzungen für diese Art von Unterfangen.

Ressource Management

Im Unternehmensumfeld wird häufig der Begriff der Ressource[1] verwendet, um mit ihm ein materielles Gut oder immaterielles Gut zu beschreiben. Als Beispiel wären hier Betriebsmittel, Rohstoffe, Geldmittel sowie die Arbeitszeit als menschliche Ressource zu nennen. IT-Ressourcen bilden eine Teilmenge des klassischen Ressourcenbildes eines Unternehmens. Um so wichtiger ist die Verwaltung dieser Ressourcen, vor allem für Entscheidungen auf dem Weg in eine Cloud, aber auch beim Ausstieg. Wird eine Cloud-Lösung verlassen und man wechselt aus dieser heraus, so kommt es besonders darauf an, ein klares Bild der erforderlichen Ressourcen zu haben, die man lokal bereit stellen muss, um darauf die bisher in der Cloud befindlichen Systeme abbilden zu können, um einen reibungslosen Betrieb sicher zu stellen.

IT-Ressourcen

Unter dem Begriff IT-Ressource versteht man im Bereich der Informationstechnologie eine Ressource, die ein Unternehmen bei Aufgaben der elektronischen Datenverarbeitung unterstützt und auf Basis der angebotenen Funktionalität wie folgt diversifiziert werden kann: (Fehling & Leymann, Gabler Wirtschaftslexikon, 2014)

Software IT-Ressourcen	IT-Ressourcen, mit denen ein Anwender direkt interagiert. Solche Ressourcen bieten komplette Anwendungen über ein Nutzerinterface an.
Plattform IT-Ressourcen	IT-Ressourcen, die von anderen Anwendungen genutzt werden. Plattform-IT-Ressourcen stellen dabei entweder Betriebsumgebungen, wie vom Anbieter verwaltete Server oder Process Engines, bereit oder bieten Anwendungsfunktionalität an, die von kundenspezifischen Anwendungen genutzt wird. Beispiele hierfür sind Abrechnungsdienste oder Mitarbeiterverzeichnisse, die z.B. als Web Service zugänglich sind.
Hardware IT-	Physikalische oder virtualisierte Server, auf denen vom Kunden verwaltete Software-IT-Ressourcen oder

[1] lat. resugere (v) hervorquellen

Ressourcen	Plattform-IT-Ressourcen installiert werden können.

Tabelle 1 - Diversifizierung von IT-Ressourcen (Fehling & Leymann, Gabler Wirtschaftslexikon, 2014)

Anhand dieser Diversifizierung können IT-Ressourcen von einem Enterprise Resource Planning System (i.d.F. ERP-System) erfasst, in entsprechende Prozesse eingebunden und deren Bedarf immanent gemessen werden. Basierend auf den individuellen Unternehmensparametern hinsichtlich des gemessenen Ressourcenbedarfs ist somit eine korrekte Skalierung dieser IT-Ressourcen gegeben, und die Gefahr der Ressourcenverschwendung durch Unterbeanspruchung bzw. übermäßige Ressourcenabnutzung durch Überbeanspruchung minimiert. Bei Abbildung von IT-Ressourcen in der Cloud ergibt sich diesbezüglich ein anderes Bild.

Cloud IT-Ressourcen – Quo Vadis?

Im vorangegangen Kapitel wurde eine Diversifizierung von IT-Ressourcen vorgestellt. Deren Hauptattribute Hardware, Plattform und Software können auf die Cloud Servicemodelle umgelegt werden. So lassen sich Hardware IT-Ressourcen auf IaaS Cloud Ressourcen, Plattform IT-Ressourcen auf PaaS Cloud Ressourcen und Software IT-Ressourcen auf SaaS Cloud Ressourcen migrieren, und somit aus dem IT-Ressourcenpool des Unternehmens trennen. Hierbei darf jedoch nicht von einer Auflösung jener IT-Ressourcen ausgegangen werden.

Für das IT-Ressource Management ist es nahezu unerheblich, ob sich die prozessintegrierten IT-Ressourcen am Firmenstandort befinden, oder in der Cloud abgebildet sind. Durch den Gang in die Cloud erhält das IT-Ressource Management zusätzliche Regelmöglichkeiten, um die Bereitstellung von IT-Ressourcen für Unternehmensprozesse unten den Gesichtspunkten Provisionierung, Messbarkeit, Kosten, Wartung, Change-Management, Update und Design elastisch zu gestalten.

Cloud IT-Ressourcen - Management

Der Gang in die Cloud beginnt im KMU Umfeld meist durch die Auslagerung unternehmensinterner E-Mail Serversysteme in eine Cloud-Lösung des Internetanbieters (i.d.F. ISP). Somit reduziert sich sowohl der unternehmensinterne Hardware IT-Ressourcen-, als auch Software IT-Ressourcenanteil. In Abwesenheit eines Ressourcenmanagementsystems schwelt bereits hier die Gefahr, mehr Cloud Ressourcen in Anspruch zu nehmen, als tatsächlich benötigt werden (Unterbeanspruchung). Aufgrund des Abrechnungsmodells von Cloud-Ressourcen kann sich eine solche Unterbeanspruchung durchaus negativ auf die entstehenden Kosten auswirken.

Cloud Ressource Management Systeme bietet in diesem Falle mehrere Werkzeuge für IT-Verantwortliche in Unternehmen, um diesen Effekten entgegenzuwirken. Diese reichen von der Einholung von Echtzeitangeboten für zusätzlich benötigte IT-Ressourcen über die Behandlung von Service Level Agreements (i.d.F. SLA) und Lebenszyklen der Ressourcen bis zur Nutzungsauswertung der bestehenden Cloud-Ressourcen.

Somit kann das Unternehmen IT-Ressourcen, welche in der Cloud abgebildet sind, sowohl effiziert als auch effektiv unter Verwendung von Ressource Management zum Einsatz bringen.

Ex Cloud – der Weg zurück

In manchen Fällen ist die Abbildung von IT-Ressourcen in der Cloud durch diverse Gründe nicht mehr möglich. In diesem Fall spielt das Cloud Ressource Management ebenfalls eine große Rolle, da basierend auf den immanent erhobenen Leistungswerten die neuerliche Bereitstellung der unternehmensinternen IT-Ressourcen korrekt skaliert werden kann.

Zusammenfassung

Sie haben nun unterschiedliche Möglichkeiten kennengelernt, wie Sie in die Cloud gehen können. Sie können sich rein der Infrastruktur eines Anbieters bedienen und sich der Belastungen durch Hardware, Stromanbindung, Klimatisierung, Backup und in höchster Ausbaustufe auch der Redundanzen (z.B. zweiter Server) entledigen. Darauf aufbauend können Sie auch ganze Dienste bei einem Anbieter anmieten, wobei die Infrastruktur für Sie hierbei nicht mehr ersichtlich ist.

Der größte Vorteil einer Cloud ist zugleich auch der größte Nachteil. Sie geben einen Teil der Verantwortung für unternehmenskritische Systeme an Dritte ab und müssen sich damit nicht mehr befassen. Dies bedeutet aber auch, dass die Abhängigkeit von diesem Anbieter hoch ist und Sie darauf vertrauen müssen, dass er die Reaktionszeiten und Verfügbarkeiten der Dienste entsprechend den Vereinbarungen auch einhält und mit Ihren gespeicherten Daten sorgsam umgeht. Es empfiehlt sich daher, auf Anbieter zu setzen, die Sie kennen und die idealerweise auch am österreichischen Markt aktiv sind und somit den österreichischen Gesetzen unterliegen. Eine Prüfung der AGBs kann in keinem Fall schaden.

Literaturverzeichnis

Accenture. (2012). *Building your Cloud Strategy with Accenture.*
Accenture. (2012). *Cloud Computing*.
Accenture. (2012). *Cloud Market Insight.*
Arbitter, P., Deutsch, P., Pracht, T., & Retti, M. (2011). Cloud Computing - mehr als nur industrialisierte IT. In C. Köhler-Schulte, *Cloud Computing: Neue Optionen für Unternehmen* (S. 35-48). Berlin: KS-Energy-Verlag.
Beckereit, F. (2011). Quo vadis Virtualisierung - Infrastrukturen für die Private Cloud. In C. Köhler-Schute, *Cloud Computing: Neue Optionen für Unternehmen* (S. 67-89). Berlin: KS-Energy-Verlag.
Brunetti, R. (2011). *Windows Azure Step by Step.* Sebastopol: O'Reilly Media.
BSI. (8. 12 2013). *Bundesamt für Sicherheit in der Informatik*.
Bundesamt für Sicherheit in der Informationstechnik - BSI. (02 2012). *Cloud Computing Eckpunktepapier.*
Bundeskanzleramt. (2012). *Österreichisches Informationssicherheitshandbuch - Cloud Strategie.* Wien: Bundeskanzleramt.
Bundeskanzleramt Rechtsinformationssystem. (2000). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, Fassung vom 13.12.2013*.
Cordial, A. (2011). *Cloud Computing: Immer in Richtung Cloud*.
Gartner Group. (2012). *Special Report Cloud Computing*.
Giedke, A. (2013). *Cloud Computing: Eine wirtschaftsrechtliche Analyse mit besonderer Berücksichtigung des Urheberrechts.* München: Herbert Utz.
Höllwarth, T. (2011). *Cloud Migration* (1. Auflage 2011 Ausg.). Heidelberg: mitp.
Halpert, B. (2011). *Auditing Cloud Computing - A Security and Privacy Guide.* (J. W. Inc., Hrsg.) CA: Wiley.
Hogan, B. (2011). *HTML5 & CSS3: Webentwicklung mit den Standards von morgen.* Köln: O'Reilly.
Hong, H. L., & Fenn, J. (21. 08 2013). *Gartner.*
IDC. (2008). *IDC eXchange*.
Krishnan, S. (2010). *Programming Windows Azure: Programming the Microsoft Cloud.* Sebastopol: O'Reilly Media.
Kuppinger, M. B. (19. 09 2012). *Cloud und BYOD fordern das Identity-Management*. From Computerwelt: http://www.computerwelt.at/news/technologie-strategie/detail/artikel/cloud-und-byod-fordern-das-identity-management/
Mörsdorf, D. (14. 07 2011). *GfK Austria.*
Masak, D. (2007). *SOA ? Serviceorientierung in Business und Software.* Wiesbaden, DE: Springer Berlin Heidelberg New York.
Mathew, J., Sarker, S., & Varshney, U. (2004). M-Commerce Services: Promises and Challenges. *Communications of the Association for Information Systems: Vol. 14* .
Meir-Huber, M. (2011). *Cloud Computing - Praxisratgeber und Einstiegsstrategien.* Wien, 2010: entwickler.press.
Metzger, C., Reitz, T., & Villar, J. (2011). *Cloud Computing - Chancen und Risiken aus technischer und unternehmerischer Sicht.* München.
Microsoft. (1. 2 2004). *Microsoft Developer Center*.
Moritz Borgmann, T. H. (2012). *On the Security of Cloud Storage Services.* Darmstadt: Fraunhofer Institue for Secure Information Technology SIT.

NACHWEIS FÜR SICHERE CLOUD: „ISO 27001 WIRD VON KUNDEN AKZEPTIERT UND VERLANGT“. (März 2013).
NIST - National Institue of Standards and Technology. (2011). *The NIST Definition of Cloud Computing*.
NIST. (1. 09 2011). *NIST National Institute of Standards and Technology.*
Patterson, L. (2010). *IBM Midmarket Software Buying and Selling Guide.* USA: IBM Redpaper.
Precht, M., Meier, N., & Tremel, D. (2004). *EDV-Grundwissen - Eine Einführung in Theorie und Praxis der modernen EDV* (7., aktualisierte Auflage Ausg.). München: ADDISON-WESLEY.
Terplan, K., & Voigt, C. (2011). *Cloud Computing.* Heidelberg, DE.
Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing - A Practical Approach.* New York, USA: McGraw-Hill.
Velte, A., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing - A Practical Approach.* US: McGraw-Hill.
Vmware Inc. (14. 12 2013). *vmware*.

Internet-Links

http://www.elektronik-kompendium.de/sites/net/0902281.htm
http://www.netzwelt.de/news/85067_5-netzwelt-wissen-ssl-verschluesselung.html
http://www.computerwoche.de/a/cloud-daten-sicher-verschluesseln,2536499
http://www.cloudsider.com/cloud-speicher
http://www.cloudcomputing-insider.de/sicherheit/content-security/articles/370196/
http://www.synology-wiki.de/index.php/Grunds%C3%A4tzliches_zum_Thema_Netzwerksicherheit
https://en.wikipedia.org/wiki/List_of_backup_software
http://www.connect.de/ratgeber/marktuebersicht-26-cloudspeicher-im-vergleich-1469235.html
http://www.cloudvergleich.net/
http://www.tecchannel.de/server/cloud_computing/2030180/cloud_computing_das_muessen_sie_wissen_saas_paas_iaas/
http://www.cio.de/was_ist_cloud_computing/2930545/
http://thejournal.com/articles/2013/10/01/the-major-cloud-computing-problems-youre-not-paying-attention-to.aspx

Präsentationen:

The dark cloud. Autoren: Florian Brunner, Thomas Kastner; Hacking Night 2012
Cloud.Lösungen im Business-Einsatz. Autor: DI Martin Schober, Vortragsreihe: IT-Sicherheit 2013
IT-Sicherheit und SaaS. Autor: DI Martin Schober; VHS-Themenabend 2013/2014

Bücher, Artikel, Zeitschriften:

Cloud Computing. C't-Magazin 6/2013
Sicherheit und die Cloud. COM-Magazin 09/2013
Backup wie von selbst. C't-Magazin 13/2013
Diplomarbeit Rüdiger Linhard
Übersicht Cloudanbieter und deren Kriterien. DI Martin Schober; August 2013