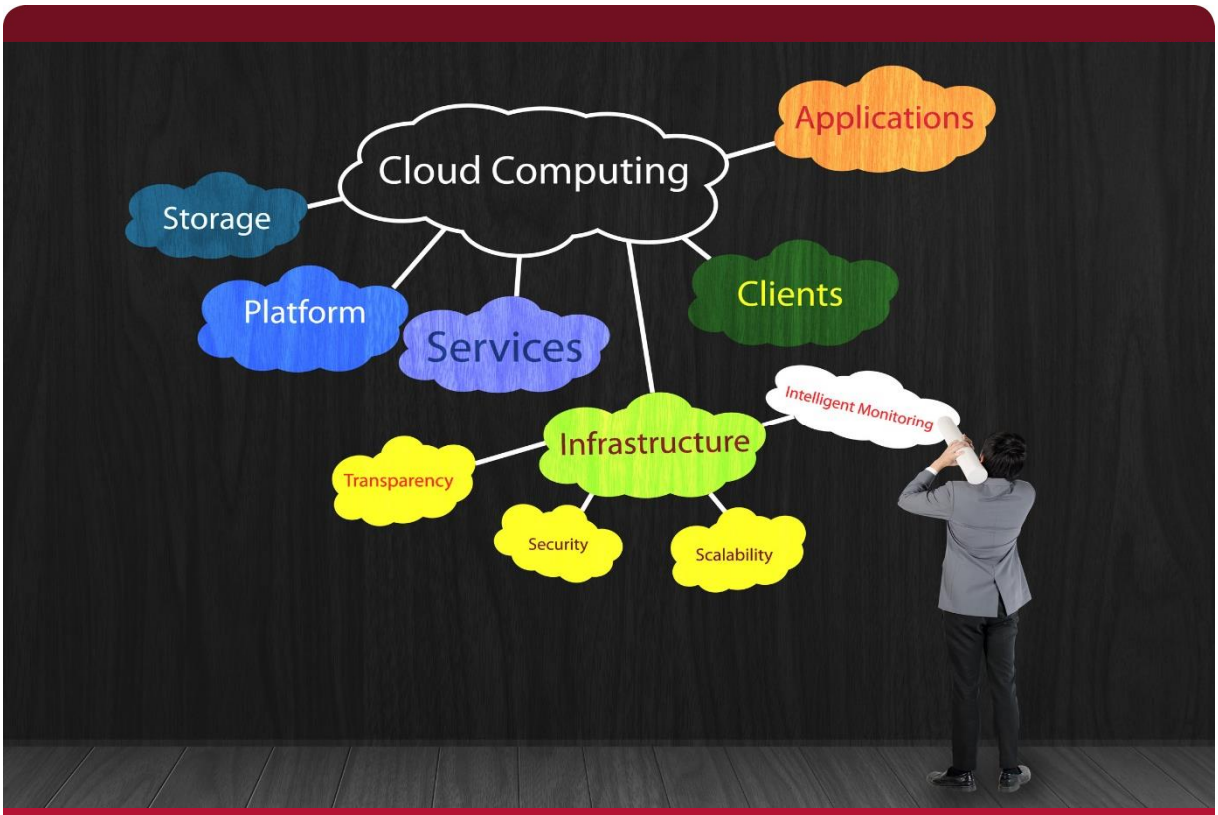
IT-Sicherheit im Handwerk



Cloud-Computing

Dozentenhandbuch

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Das diesem Buch zugrundeliegende Verbundvorhaben "IT-Sicherheitsbotschafter im Handwerk - qualifizierte, neutrale Botschafter für IT-Sicherheit im Handwerk finden, schulen und Awarenesskonzepte erproben (ISiK)" wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen der Task Force "IT-Sicherheit in der Wirtschaft" gefördert und durch den Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR) betreut.
Die Task Force "IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind unter: *www.it-sicherheit-in-der-wirtschaft.de* abrufbar.

Herausgeber:

Institut für Technik der Betriebsführung (itb) im
Deutschen Handwerksinstitut (DHI) e.V.
Kriegsstraße 103a Å76135 Karlsruhe (Konsortialführer)

Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET) der
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz (fachliche Leitung)

Westfälische Hochschule
Institut für Internet-Sicherheit ï if(is)
Neidenburger Straße 43 • 45877 Gelsenkirchen
(Kooperationspartner)

Interessengemeinschaft des Heinz-Piest-Instituts für Handwerkstechnik (HPI) an der Leibniz-Universität Hannover
Wilhelm-Busch-Straße 18 • 30167 Hannover
(Kooperationspartner)

Das Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung und des Nachdrucks, bleiben, auch bei nur auszugsweiser Verwertung vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Herausgeber reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.
Text, Abbildung und Programme wurden mit größter Sorgfalt erarbeitet. Die Autorinnen und Autoren können jedoch für eventuell verbleibende fehlerhafte Angaben und deren Folgen weder eine juristische noch irgendeine andere Haftung übernehmen.

ISBN **978-3-944916-08-8**

Verlag: Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
www.hwk.de

© 2014 Projekt ISiK, 1. Auflage

Autorenteam

Falk Gaentzsch

Bachelor of Science und wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit ï if(is) an der Westfälischen Hochschule in Gelsenkirchen. Projektleiter für das Projekt ĂT-Sicherheit im Handwerkñ

Schwerpunkte:
IT-Sicherheit & Awareness
Cloud-Computing
Virtualisierung

Prof. Norbert Pohlmann

Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen.

Einleitung

Seit dem Cloud-Computing in Deutschland an Bedeutung gewonnen hat, ist es ein vielfach diskutiertes Thema in allen Branchen, von der hoch spezialisierten IT-Branche bis hin zu Handwerksunternehmen.

Ein maßgebliches Argument für Cloud-Computing ist das Einsparpotenzial bei den Kosten in der Verwaltung und Wartung der Unternehmens-IT. Ein weiteres Beispiel für eine Reduzierung der Kosten ist ein geringerer Energieverbrauch, weil Server nicht im eigenen Unternehmen untergebracht werden müssen. Ebenso kann durch eine bessere Vernetzung der Anwendungen in der Cloud die Mitarbeiterkommunikation erhöht und damit die Produktivität gesteigert werden.

Ein Einstieg in die Cloud sollte jedoch nicht erfolgen, ohne alle Risiken über diese Technologie in Betracht gezogen zu haben.
Größte Hindernisse für potenzielle Kunden sind unter anderem Bedenken bei dem Thema Datenschutz, weil Unternehmensdaten einem externen Cloud-Service-Provider (CSP) anvertraut werden. Gleichermaßen machen sich Cloud-Nutzer Sorgen um die Sicherheit und Verfügbarkeit ihrer Daten.

Viele Unternehmen sehen den Datenschutz bei Cloud-Unternehmen nicht hinreichend gewährleistet Dies trifft ausschließlich bei außereuropäischen Cloud-Anbietern zu, bei denen kein europäischer Datenschutzstandard gesetzlich gewährleistet wird.
Dieser Fakt ist ein deutlicher Vorteil für Cloud-Computing im Europäischen Wirtschaftsraum. Viele Unternehmen vertrauen in Folge der aktuellen Entwicklungen rund um den NSA-Skandal nur noch Unternehmen und Datenzentren in Europa. Diese Annahme kann aus Umsatzrückgängen bei US-Cloud-Anbietern geschlossen werden, die sich auf circa 10 bis 20% beziffern lassen (Sylvia Beckers, 2013).
Aus diesen Gründen und durch steigende Nutzerzahlen ist damit zu rechnen, dass die Preise für Cloud-Computing im Europäischen Wirtschaftsraum und in Deutschland sinken werden.

Eine weitere Gefahr entsteht, wenn Daten in das Visier von Hackern geraten. Diese sehen die Chance, gerade bei großen Cloud-Service-Providern eine hohe Datenmenge erbeuten zu können, insbesondere wenn dort eklatante Schwachstellen in den Softwaresystemen zu finden sind. Industriespionage und Wirtschaftsspionage könnten weitere Ziele von Angreifern sein, dabei sind beispielsweise Konstruktionspläne, Gebäudepläne und die Auftragslage nicht nur in großen Unternehmen, sondern auch in Handwerksbetrieben im Fokus von Hackern. Dies trifft besonders auf Handwerksunternehmen zu, die Aufträge bei großen Unternehmen ausführen, diese können für Angreifer als Informationsquelle oder Sprungbrett für gezielte Angriffe genutzt werden.

Mit Hilfe von Beispielen soll in diesem Handbuch eine grundlegende Übersicht über Sicherheitsmechanismen dargestellt werden. Ebenso werden Argumente für und gegen die Nutzung von Cloud-Computing aufgeführt, mit deren Hilfe eine Entscheidung im Unternehmen in Bezug auf Cloud-Computing getroffen werden kann.

Anmerkung zu den Beispielen in diesem Handbuch

Die Betriebe, Angriffsszenarien und Schadensbeispiele in diesem Handbuch sind frei erfunden und sollen nur die möglichen Auswirkungen von Fehlern und Angriffen verdeutlichen.

Seminarziele

Das Ziel dieses Handbuches ist es, ein Grundverständnis für die Vor- und Nachteile von Cloud-Computing, in Bezug auf die IT-Sicherheit des Unternehmens, zu vermitteln. Die Erkenntnisse in diesem Handbuch basieren auf dem aktuellen Wissensstand rund um das Thema Cloud-Computing.

Am Ende dieses Seminars sind Sie in der Lage:

- Grundlagen über das Thema Cloud-Computing vermitteln zu können.
- Vorteile und Risiken von Cloud-Computing darzustellen.
- Bei der Entscheidungsfindung rund um das Thema Cloud-Computing zu unterstützen.
- Geeignete Cloud-Dienste zu identifizieren und von unpassenden Angeboten abzuraten.
- Sicherheitsempfehlungen bei der Nutzung von Cloud-Diensten auszusprechen.

Inhaltsverzeichnis

AUTORENTEAM ..... **III**

EINLEITUNG ..... **IV**

SEMINARZIELE ..... **V**

INHALTSVERZEICHNIS ..... **VI**

1. Cloud-Computing **1**
1.1 Was ist Cloud-Computing? 1
1.2 Merkmale von Cloud-Computing 1
1.3 Realisierung von Cloud-Computing 2
1.3.1 Infrastructure as a Service (IaaS) 3
1.3.2 Platform as a Service (PaaS) 3
1.3.3 Software as a Service (SaaS) 4
1.4 Organisation der Cloud 4
1.4.1 Public-Cloud 5
1.4.2 Private-Cloud 5
1.4.3 Hybrid-Cloud 6
1.4.4 Community-Cloud 6
1.5 Technische Realisierungen von Cloud-Lösungen 7
1.5.1 Public-Cloud ï Infrastructure as a Service 7
1.5.2 Private-Cloud ï Infrastructure as a Service 8
1.5.3 Infrastructure as a Service ï Risiken 9
1.5.4 Public-Cloud ï Software as a Service 9
1.5.5 Private-Cloud ï Software as a Service 9
1.5.6 Software as a Service ï Risiken 10
1.6 Verbreitung von Cloud-Computing im Handwerk 10
1.7 Vorteile von Cloud-Computing 11
1.7.1 Kosten 11
1.7.2 Know-how in puncto IT-Sicherheit nutzen 12
1.7.3 Bedarfsgerechter Einsatz 12
1.7.4 Wartungsaufwand 12
1.7.5 Skalierbarkeit und Flexibilität 13
1.7.6 Hohe Verfügbarkeit 13
1.8 Nachteile von Cloud-Computing 13
1.8.1 Abhängigkeit 13
1.8.2 Netzzugang und Arbeitsgeschwindigkeit 14
1.8.3 Funktionsumfang 14
1.8.4 Verlässlichkeit 15
1.8.5 Skalierung und mögliche Folgen 15
1.9 Zusammenfassung 16

2. Risiken bei der Nutzung von Cloud-Computing **17**
2.1 Möglicher Verlust der Datenhoheit 17
2.2 Unternehmerischer Datenmissbrauch 17
2.2.1 Viren und Schadsoftware in der Cloud 18
2.2.2 Hacken und Cloud 18
2.3 Kritische Handlungsfelder in der Cloud 19
2.3.1 Verlust der Verfügbarkeit bei Totalausfällen 19
2.3.2 Insolvenz eines Cloud-Anbieters 19
2.3.3 Vendor Lock-in (Anbieterabhängigkeit) 20

2.4 Zusammenfassung ... 20

3. Basisschutz: Handlungsempfehlungen ... 21
3.1 Basisschutz auf Geräten ... 21
3.1.1 Updates ... 21
3.1.2 Sichere Passwörter ... 21
3.1.3 Security-Suiten ... 22
3.2 Zugriff auf Cloud-Ressourcen ... 23
3.2.1 Verschlüsselungstechniken bei der Datenübertragung ... 23
3.2.2 Zugriff von mobilen Geräten (BYOD) ... 24
3.2.3 Verschlüsselung ... 24
3.2.4 Benutzergruppen-Management inkl. Rechte-Management ... 26
3.3 Zusammenfassung ... 26

4. Cloud-Computing im Handwerk ... 27
4.1 Anwendungsmöglichkeiten einer Cloud im Handwerksbetrieb ... 27
4.1.1 Software as a Service ï Handwerkslösungen: Positives Beispiel ... 27
4.1.2 Software as a Service ï Handwerkslösungen: Negatives Beispiel ... 28
4.1.3 Resümee der Beispiele ... 29
4.1.4 Einzelne Dienstleistungen/Services aus der Cloud ... 30
4.2 SaaS für Handwerksunternehmen ... 31
4.2.1 Weka Handwerksbüro ... 31
4.2.2 Lexoffice ... 32
4.3 Leitfaden zur Entscheidungsfindung ... 34
4.3.1 Auswahl Cloud-Anbieter ... 34
4.3.2 Zertifizierungen für Cloud-Dienste und ihre Bedeutung ... 35
4.3.3 Mitarbeiter-Sensibilisierung ... 39
4.4 Zusammenfassung ... 40

5. Compliance & Recht ... 41
5.1 Vertragsrechtliche Bestimmungen ... 41
5.1.1 Allgemeine Geschäftsbedingungen (Leistungsschuld) ... 41
5.1.2 Lizenzierung von Software in der Cloud ... 41
5.2 Service Level Agreement ... 42
5.2.1 Was ist bei Service Level Agreements zu beachten? ... 43
5.2.2 Klassifizierung SLA ... 43
5.3 Was ist beim Anbieterwechsel zu beachten? ... 44
5.3.1 Rückgabeformat der Daten bei Vertragsbeendigung ... 44
5.3.2 Daten komplett aus der Cloud löschen ... 45
5.4 Einheitliche Standards für Cloud-Computing ... 45
5.5 Datenschutzrechtliche Anforderungen ... 45
5.5.1 Datenschutz in Deutschland und Europa ... 45
5.5.2 Datenschutz außerhalb Europas ... 46
5.6 Zusammenfassung ... 48

6. Checkliste ĂCloud-Computingñ ... 49

7. Weblinks ... 51

8. Literaturverzeichnis ... 52

9. Stichwortverzeichnis ... 54

10. Abbildungsverzeichnis ... 57

1. Cloud-Computing

In diesem Kapitel wird ein fundiertes Basiswissen zum Thema Cloud-Computing dargestellt Dies umfasst die grundlegenden Merkmale von Cloud-Computing, sowie Modelle und Möglichkeiten, wie Cloud-Computing realisiert und genutzt werden kann.

1.1 Was ist Cloud-Computing?

Zu erklären was Cloud-Computing bedeutet, ist gar nicht so schwierig, wenn Sie sich vorstellen, dass viele von uns Cloud-Computing nutzen, ohne es überhaupt zu ahnen. Wenn wir die Komplexität der Strukturen zunächst außen vor lassen, können Sie sich zum Beispiel einen E-Mail-Dienst vorstellen, der von einem Dienstleister angeboten wird. Bei diesem Beispiel wird nach heutiger Ansicht bereits von einem Cloud-Service gesprochen. Es werden demnach Ressourcen und eine Anwendungslogik von einem Cloud-Service-Provider (CSP) bereitgestellt. Der Nutzer kann bei seinem Cloud-Anbieter verschiedene Dienste wie beispielsweise Anti-Spam oder Virenschutz hinzu oder wieder abbuchen, ebenso kann der Speicherplatz (Storage as a Service) im genutzten Postfach von einem grundlegend angebotenen Basisniveau individuell erhöht und angepasst werden. Alle durch den Nutzer verwendeten Zusatzdienste werden monatlich in einem Abonnement-Modell abgerechnet.

Bei Cloud-Computing werden Ressourcen, wie beispielsweise Arbeitsspeicher, Festplattenspeicher und Rechenkapazität, bei einem Cloud-Service-Provider genutzt.

Die Verwendung eines Cloud-Dienstes kann über Internet-Browser (zum Beispiel Mozilla Firefox, Google Chrome oder Microsoft Internet Explorer) realisiert werden. Dabei ist es irrelevant, ob der Nutzer für den Zugriff auf den Cloud-Dienst einen Computer oder ein Mobiltelefon verwendet. Alternativ kann auch eine Software genutzt werden, die auf einem lokalen Gerät installiert wird. Dies bietet die Möglichkeit, die Nutzung für einen Anwender komfortabler zu gestalten.

Auf Cloud-Dienste kann mittels Smartphone oder PC, per Applikation oder über einen Browser zugegriffen werden.

1.2 Merkmale von Cloud-Computing

Durch das National Institute of Standards and Technology wurden folgende charakteristischen Merkmale definiert (NIST-Computer Security Division, 2011):

- **Bedarfsgerechte Selbstverwaltung von Services:**
  Konsumenten können sich bei Bedarf Kapazitäten wie Rechenzeit auf Servern und Netzwerkspeicher ohne zusätzliche Interaktion mit einem menschlichen Mitarbeiter selbst buchen.
- **Umfassender Netzwerkzugriff:**
  Ressourcen sind standardisiert über das Netzwerk mit gängigen Mitteln, zum Beispiel mit Smartphone, Laptop oder Desktop-PC, verfügbar.
- **Ressourcen-Bündelung:**
  Die Ressourcen eines Service-Anbieters sind gebündelt und ermöglichen es, mehrere Kunden in einem Mehrnutzermodell zu bedienen. Dabei wissen einzelne Kunden nicht zu jedem Zeitpunkt, wo sich die bereitgestellten Ressourcen befinden. Es kann jedoch abstrakt festgelegt werden, wo sich diese Ressourcen befinden sollen, zum Beispiel in einem bestimmten Land oder in einem speziellen Rechenzentrum. Ressourcen sind beispielsweise Arbeitsspeicher, Rechenzeit, Netzwerkbandbreite und Festplattenspeicher.

Merkmale von Cloud-Computing sind: bedarfsgerechte Selbstverwaltung von Services, umfassender Netzwerkzugriff, Ressourcen-Bündelung und dynamische Anpassungsfähigkeit.

- **Dynamische Anpassungsfähigkeit:**
  Kapazitäten können elastisch angefordert und freigegeben werden, in einigen Fällen automatisch, um schnell durch Skalierung mögliche Schwankungen beim eingehenden oder ausgehenden Bedarf abfangen zu können.

Die Servicequalität kann mittels Service-Level-Agreement vereinbart und durch den Nutzer anhand von Kennzahlen geprüft werden.

Zusätzlich zu einem allgemeinen Vertrag zwischen Anbieter und Nutzer wird ein Service Level Agreement (SLA) erarbeitet (siehe Kapitel 5.2). In einem SLA wird festgelegt, zu welchen Bedingungen und mit welcher Qualität die Dienste durch einen Cloud-Service-Provider bereitgestellt werden müssen.

Jede neue Technologie birgt auch Risiken, die in Kapitel 2 dargestellt werden.

1.3 Realisierung von Cloud-Computing

Bei der Realisierung von Cloud-Computing wird zwischen drei verschiedenen Ebenen unterschieden. Die folgenden Realisierungs-Modelle bilden die grundlegende Nutzungsstruktur für Cloud-Computing:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Cloud-Computing-Modelle sind IaaS, PaaS und SaaS.

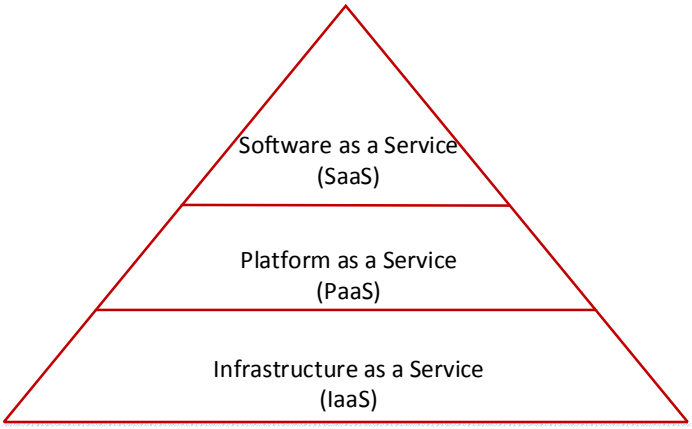


Abbildung 1: Realisierung von Cloud-Computing

Die API im PaaS-Modell kann genutzt werden, um eigene Programme in der Cloud zu entwickeln und um bestehende Programme anzupassen.

Für die Verwaltung einer Cloud-Lösung stellt der Cloud-Service-Provider eine Administrationsoberfläche in einem Internetportal bereit. In diesem Portal können Ressourcen individuell abgestimmt werden.
Sind Programmierkenntnisse vorhanden kann zusätzlich das ĂApplication Programming Interface (API)ñdes jeweiligen Anbieters genutzt werden, um eigene Anpassungen und Programme zur Verwaltung der Cloud-Infrastruktur erstellen und verwenden zu können. Mit der API ist es möglich, Applikationen direkt für die jeweils genutzte Cloud-Umgebung zu konzipieren, sodass auch andere Nutzer einer Cloud diese nutzen oder sogar erwerben können. Diese Anwendungen werden in einem App-Store bereitgestellt und jeder Administrator in einem Handwerksunternehmen kann diese für die jeweilige Cloud-Lösungen kostenfrei oder gegen eine Gebühr installieren.

In den folgenden Abschnitten werden die Cloud-Computing-Modelle näher betrachtet.

1.3.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service ist die Basis aller Cloud-Strukturen. Auf dieser Ebene wird Hardware, in den Rechenzentren der Cloud-Service-Provider, virtualisiert. Alle für ein Computernetzwerk nötigen Komponenten wie zum Beispiel Festplattenspeicher, Prozessoren, Arbeitsspeicher und Netzwerkkomponenten sowie virtuelle Switches und Router können für die Nutzer ressourcensparend bereitgestellt werden.

Für weitere Informationen zu diesem Thema Virtualisierung nutzen Sie bitte das Handbuch Virtualisierung oder entsprechende Fachliteratur.

Cloud-Computing bietet die dynamische Anpassung von Ressourcen (Prozessor, Arbeitsspeicher und Festplattenspeicher).

Stellen sie sich vor, dass zu einer gewissen Stoßzeit ein hohes Nutzeraufkommen auf Ihrer Internetseite stattfindet. Server-Administratoren werden bei diesem Gedanken nervös. Cloud-Nutzer können gelassen bleiben, haben sie doch ihre automatische Ressourcenskalierung aktiviert. Hierbei wird bei Bedarf ab einer festgelegten Auslastungsgrenze einfach mehr Speicher dynamisch zu den bestehenden Ressourcen hinzugebucht. Das Gleiche passiert, wenn eine Erhöhung des Festplattenspeichers nötig wird. In dieser Situation wird dynamisch mehr Speicher angefordert und am Monatsende im Abonnement verrechnet.
Dies sind die neuen Möglichkeiten, die sich durch Cloud-Computing ergeben. Wenn ganze Serversysteme vermietet werden, muss ein Servicemitarbeiter Festplatten per Hand hinzufügen, falls Auslastungsgrenzen erreicht werden. Dieser Schritt wird heutzutage per Mausklick durch den Nutzer selbst oder durch ein automatisches Ressourcenmanagement ausgeführt.

1.3.2 Platform as a Service (PaaS)

Platform as a Service bietet eine Entwicklungsumgebung, die maßgeblich für die Programmierung von Anwendungen und Webapplikationen genutzt werden kann. Daher ist diese Ebene oft nicht direkt für Handwerksunternehmen relevant, allerdings sollte dieser Service erwähnt werden, damit die Möglichkeiten bei der Verwendung von Cloud-Computing weiter verdeutlicht werden.

PaaS ist eine Entwicklungs-umgebung, die benötigte Hardware wird durch einen Cloud-Service-Provider bereitgestellt.

Ein Programmierer muss sich bei der Nutzung von Platform as a Service nicht um die Wartung oder Neuanschaffung der genutzten Hardware-Ressourcen in der Cloud sorgen. Die Hardware wird von einem Cloud-Service-Provider gepflegt und gewartet. Die Kapazitäten der verwendeten Plattform werden virtualisiert vom Cloud-Service-Provider durch die Verwendung von Infrastructure as a Service bereitgestellt, Platform as a Service setzt auf genau diese Ressourcen auf.
Es ist möglich, Lizenzen für neue Nutzer oder Programmierer monatlich zum bestehenden System hinzuzubuchen.
Entwickler können Kollaborations-Tools direkt aus der Cloud verwenden, um mit anderen Entwicklern zu kommunizieren und sich über neue Entwicklungsmeilensteine auszutauschen. Problematisch wird es, wenn die entwickelten Applikationen auch auf App-Stores von anderen Cloud-Anbietern bereitgestellt werden sollen. Dies scheitert zumeist an der fehlenden Kompatibilität zwischen verschiedenen Cloud-Service-Providern.

1.3.3 Software as a Service (SaaS)

Für Software as a Service ist ein schneller Internetzugang nötig, der mindestens eine DSL-Geschwindigkeit aufweisen sollte.

Bei Software as a Service wird eine Anwendung von einem Cloud-Service-Provider bereitgestellt. Diese kann beispielsweise aus den Bereichen der Lagerverwaltung, Kundenverwaltung oder Lohnverwaltung kommen, um nur einige Einsatzmöglichkeiten zu nennen.
Bei einer hochwertigen und leistungsstarken Cloud-Lösung sollte ein Anwender gar nicht bemerken, ob er gerade eine Anwendung auf dem lokalen System oder in der Cloud ausführt, dabei muss auch auf einen schnellen Internetzugang geachtet werden. Der Nutzer muss sich lediglich mit seinen Nutzerinformationen anmelden und hat alle Daten zur Verfügung, die eventuell kurz zuvor im Zug, beispielsweise auf einem Smartphone bearbeitet wurden.

Auch Software as a Service wird virtuell auf der Infrastruktur des Cloud-Service-Providers bereitgestellt, ebenso ist der Anbieter für die Wartung, Pflege und Absicherung der Software sowie der nötigen Hardwarekomponenten verantwortlich.

Muss eine Software installiert werden, ist der Nutzer selbst für die Aktualisierung verantwortlich.

Der Nutzer selbst hat lediglich für die Aktualität der möglichen Client-Software zu sorgen, wenn diese zum Einsatz kommt.
Die Lizenzen können sehr einfach von einem Nutzer mit Administrator-Rechten auf dem Selbstservice-Portal des Anbieters verwaltet werden. Dieser Administrator ist ebenso für die Erstellung und Löschung der verschiedenen Nutzer verantwortlich.
Für Software as a Service entstehen Kosten, wie auch in allen zuvor erwähnten Service-Modellen und sind in einem monatlichen Abonnement vom Unternehmen zu verrichten.

CAD-Arbeitsplätze können in die Cloud ausgelagert werden.

Ein Beispiel für eine SaaS-Anwendung ist Ăcadcloudñ der Firma Solid System Team GmbH. Bei dieser Cloud-Anwendung werden sehr rechenintensive CAD[1]-Arbeitsplätze in die Cloud ausgelagert. So wird es möglich auch von leistungsschwächeren Arbeitsplätzen oder von mobilen Geräten auf CAD-Anwendungen zugreifen zu können.

1.4 Organisation der Cloud

Die allgemeine Organisation von Cloud-Computing gliedert sich abstrakt in zwei Hauptfelder:

Cloud-Computing wird in den Formen Public- und Private-Cloud organisiert

- Public-Cloud
- Private-Cloud

Dabei wird unterschieden auf welchen Cloud-Ressourcen Anwendungen oder Hardwarekapazitäten verwendet werden. Bei der Nutzung einer Public-Cloud werden ausschließlich Ressourcen von einem Cloud-Service-Provider in Anspruch genommen, die sich mit anderen Cloud-Nutzern geteilt werden müssen. Darüberhinaus sind Public-Cloud-Dienste für jedermann zugänglich.
Die Verwendung einer Private-Cloud hingegen beschreibt die Nutzung von Kapazitäten auf einem Server, der ausschließlich durch das eigene Unternehmen genutzt wird. Ressourcen in dieser Organisationsform müssen demnach nicht mit anderen Mietern oder Kunden geteilt werden.

[1] *CAD* ï computer-aided design, zu Deutsch rechnerunterstütztes Konstruieren

Des Weiteren wird zwischen folgenden speziellen Cloud-Typen differenziert, die in den folgenden Kapiteln weiter beschrieben werden:

- Hybrid-Cloud
- Community-Cloud

1.4.1 Public-Cloud

In der Public-Cloud werden Ressourcen bei einem Anbieter genutzt, diese müssen mit anderen Kunden geteilt werden.

Die Public-Cloud beschreibt allgemein die Ressourcen, die in einem Rechenzentrum eines Cloud-Service-Providers bereitgestellt werden. Diese Ressourcen werden zwischen den verschiedenen Kunden auf einer so genannten Multi-Tenant-Architektur (Ätenantõ, dt. Mieter) aufgeteilt. Mit dieser Technologie ist es möglich, dass sich dutzende Kunden einen einzelnen Server bei einem Cloud-Service-Provider teilen. Dabei kommt es nicht darauf an, ob diese Anwendungen (Software as a Service) oder virtuellen Infrastruktur-Komponenten (IaaS) verwenden (Fraunhofer IESE, 2011). Auch kann nicht ausgeschlossen werden, dass ein virtueller Festplattenspeicher möglicherweise in einem anderen Bereich des Rechenzentrums verwendet wird, dieser Fakt birgt jedoch keine Nachteile und ist bei Cloud-Computing oft die Regel.
Der Cloud-Service-Provider sorgt dafür, dass jeder Nutzer auf der Infrastruktur sicher von anderen Kunden getrennt ist, um ein grundlegendes Sicherheitsniveau gewährleisten zu können. Dieses wichtige Kriterium wird als Mandantenfähigkeit (BITKOM, 2009) bezeichnet und bedeutet, dass sich Ressourcen einzelner Kunden nicht mit denen anderer Kunden überschneiden, es findet eine sichere Abgrenzung der Daten voneinander statt.

1.4.2 Private-Cloud

In der Private-Cloud werden Ressourcen nur durch das eigene Unternehmen genutzt.

Private-Cloud-Computing bietet Unternehmen die Möglichkeit ihre eigenen oder extern angemieteten Hardwareressourcen effektiver nutzen zu können. Wichtig ist hierbei, dass ein Server nicht mit einem anderen Kunden geteilt wird. Ein Nutzer hat vielmehr die volle Kontrolle über einen Server.

Die Private-Cloud ist wartungsintensiver als Services aus der Public-Cloud und benötigt ein hohes Niveau an IT-Fachwissen bei der Administration.

Der Aufwand und die Kosten bei der Verwendung einer Private-Cloud sind jedoch weitaus höher als bei der Verwendung von Public-Cloud-Diensten, da ein Unternehmen selbst für die Verwaltung und die Aktualität der Software und des Betriebssystems verantwortlich ist. Hierfür werden Mitarbeiter benötigt, die speziell für solche Wartungsaufgaben geschult werden müssen. Diese sollten sich besonders im Bereich der IT-Sicherheit auskennen, um gegen die täglichen Angriffe und Zugriffsversuche aus dem Internet gewappnet zu sein.
Stehen keine gut geschulten Mitarbeiter aus dem eigenen Unternehmen zur Verfügung, müssen wiederum Wartungs- und Installationstätigkeiten an Fremdunternehmen ausgelagert werden. Für einen Servicevertrag müssen weitere Kosten einkalkuliert werden.

Durch die Komplexität der Wartung einer Private-Cloud-Infrastruktur, ist diese nicht als Lösung für kleine Handwerksunternehmen zu empfehlen, insbesondere wenn kein ausreichendes IT-Sicherheitsniveau gewährleistet werden kann. Dies könnte zu Risiken durch fehlende Sicherheitsupdates oder zu falschen Konfigurationen führen. Unbekannte Dritte könnten Sicherheitslücken nutzen, um ein System zu manipulieren oder gar vollständig zu übernehmen.

In der Private-Cloud sind Daten unter Ihrer Kontrolle.

Einen maßgeblichen Sicherheitsvorteil gibt es jedoch bei der Nutzung einer sehr gut gewarteten und abgesicherten Private-Cloud-Infrastruktur: Daten müssen nicht externen Dienstleistern anvertraut werden, dieser entscheidende Vorteil gewinnt durch Spionageskandale in den Medien noch weiter an Bedeutung.

1.4.3 Hybrid-Cloud

Der Name der Hybrid-Cloud begründet sich aus der Mischung von Private- und Public-Cloud. Das Modell der Hybrid-Cloud ist daher eine Mischform im Cloud-Computing.

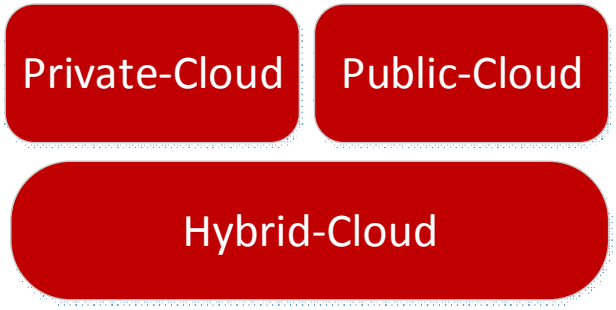


Abbildung 2: Darstellung einer Hybrid-Cloud

Bei der Hybrid-Cloud werden die Vorteile von Privat- und Public-Cloud genutzt.

Die Verwendung einer Hybrid-Cloud ist sinnvoll, denn es können jeweils die Vorteile einer Public-Cloud und einer Private-Cloud genutzt werden.
Wenn kritische Daten, das heißt vertrauliche Informationen mit hohem Schutzbedarf, in die Cloud ausgelagert werden, sollte dies nur in der eigenen Private-Cloud erfolgen. Daten mit hohem Schutzbedarf könnten beispielsweise persönliche Mitarbeiterinformationen, also personenbezogene Daten sein.

Um dieses Problem zu umgehen, sollten kritische Daten datenschutzkonform in einer Private-Cloud oder auf einem angemieteten Server innerhalb der Infrastruktur eines Handwerkunternehmens redundant, das heißt mehrfach gespeichert werden. Daten mit geringerem Schutzbedarf können hingegen in der Public-Cloud abgelegt werden.

1.4.4 Community-Cloud

Eine Community-Cloud ist der Verbund von Private-Cloud-Lösungen.

Charakteristisch für die Verwendung einer Community-Cloud ist, dass mehrere Cloud-Lösungen miteinander verknüpft werden. Teilnehmer dieser Community-Cloud können Handwerksunternehmen mit gleichen Bedürfnissen oder Tätigkeitsfeldern sein.

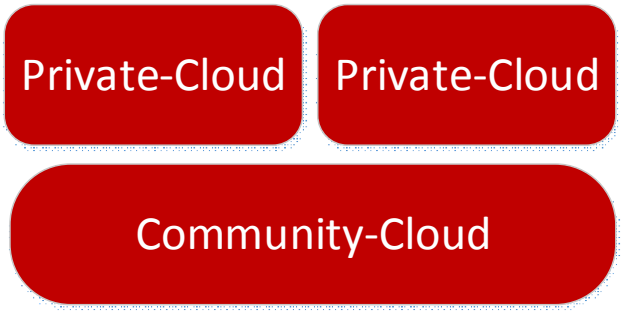


Abbildung 3: Darstellung einer Community-Cloud

Community-Cloud-Lösungen können beispielsweise durch einen Branchenanbieter realisiert werden.
Vorteile aus dieser Verwendung sind, dass Ressourcen bei Community-Cloud-Angeboten dynamisch für alle Teilnehmer desselben Cloud-Verbundes freigegeben werden können.
Kosteneinsparungen und Wissenstransfer können Synergieeffekte dieser Lösung sein. Dies bedeutet, wenn viele Handwerksunternehmen eine Community-Cloud-Lösung nutzen, sinken die Kosten und alle Unternehmen profitieren durch diesen Verbund.

1.5 Technische Realisierungen von Cloud-Lösungen

In diesem Kapitel werden Vor- und Nachteile einzelner Cloud-Lösungen dargestellt. Dabei werden die Nutzungsmöglichkeiten von Infrastructure as a Service und Software as a Service in den Bereichen von Public-Cloud und Private-Cloud dargestellt.

Die Verwendung von Platform as a Service findet hier keine weitere Erwähnung, da diese Form von Cloud-Computing nicht im Einsatzbereich von Handwerksunternehmen gesehen wird.

1.5.1 Public-Cloud ï Infrastructure as a Service

Im Folgenden werden grundlegende Vor- und Nachteile von Infrastructure as a Service im Bereich der Public-Cloud dargestellt. Beispielsweise kann es sich um die Nutzung von einem virtualisierten Cloud-Server handeln, auf dem eine Internetseite genutzt werden soll.

Beispiel:
Ein Handwerksunternehmen nutzt einen Server in der Public-Cloud, um günstig und flexibel Hardware eines Cloud-Service-Providers nutzen zu können. Auf diesem Server lassen sich Anwendungen installieren, welche so dem Personal bereitgestellt werden kann.

Vorteile

- Keine Kosten für die Unterbringung von Server-Hardware.
- Keine Errichtungskosten für Hardware.
- Kein Wartungsaufwand für Hardware in der Cloud.
- Geringere Stromkosten.

- Vorteile durch die Nutzung professioneller Rechenzentren.
- Bei IaaS lassen sich Server über Verwaltungssoftware konfigurieren.
- Hohe Verfügbarkeiten.
- Es gibt die Möglichkeit auf zertifizierte Rechenzentren zu setzen, die ein geprüftes Informationssicherheits-Managementsystem einsetzen (siehe Kapitel 4.3.1)

Nachteile

- Der Zugriff auf die Webschnittstelle ist öffentlich verfügbar und wird nur über die Passwortqualität des Administrators geschützt.
- Installierte Software muss selber gewartet werden.
- Die Komplexität der Wartung von Softwarekomponenten wie dem Betriebssystem von IaaS übersteigt oft das Know-how von Handwerksunternehmen.

1.5.2 Private-Cloud ï Infrastructure as a Service

Durch Virtualisierung können auf einem Server mehrere Betriebssysteme auf derselben Hardware emuliert und betrieben werden.

Im Folgenden werden grundlegende Vor- und Nachteile von Infrastructure as a Service im Bereich der Private-Cloud dargestellt.

Beispiel:
Ein Handwerksunternehmen betreibt einen Server im eigenen Unternehmen. Es können durch Virtualisierung verschiedene virtuelle Server mit unterschiedlichen Betriebssystemen erstellt werden.

Vorteile

- Die Datenhoheit (siehe Kapitel 2.1) bleibt im eigenen Unternehmen.
- Ressourcen können durch Virtualisierung besser genutzt und ausgelastet werden.
- Die Ausfallsicherheit durch Virtualisierung steigt.

Nachteile

- **Der Aufwand ist für Handwerksunternehmen ohne Wartungsauftrag kaum zu bewältigen.**
- Hohe Kosten bei der Anschaffung von Hardware.
- Für hohe Verfügbarkeiten müssen hohe Kosten in Kauf genommen werden siehe Kapitel 1.7.6.
- Hoher Aufwand bei der Wartung der Server.
- Es ist viel Know-how für eine sichere Konfiguration der Software und Wartung der Hardware nötig.
- Aufwand bei Auswertung der Systemereignisse (Log-Auswertung).
- Kosten für gut ausgebildetes Personal.
- Backup und Notfallstrategien müssen selbst erarbeitet und durchgesetzt werden.

1.5.3 Infrastructure as a Service ï Risiken

Ein mögliches Risiko ergibt sich, wenn einzelne Unternehmen, die die gleiche Hardware bei Infrastructure as a Service nutzen, in das Fadenkreuz von Hackern geraten. Es ist möglich, dass Angreifer versuchen könnten, die Ressourcen der virtuellen Umgebung so zu belasten, dass dies zur Überlastung führt und alle weiteren Kunden in Mitleidenschaft gezogen werden.

Aus Gründen der Datenspionage, in Ländern außerhalb des Europäischen Wirtschaftsraumes (EWR), fragen sich viele Nutzer, ob diese Art von Cloud-Computing in der Zeit der Datenspionage noch sicher ist.

Nutzen Sie Cloud-Service-Provider mit dem Hauptsitz im Europäischen Wirtschaftsraum oder in Deutschland.
Weitere Risiken finden Sie im Kapitel 2.

1.5.4 Public-Cloud ï Software as a Service

Im Folgenden werden grundlegende Vor- und Nachteile von Software as a Service im Bereich der Public-Cloud dargestellt.

Beispiel:
Ein Handwerksunternehmen nutzt eine Branchensoftware in Form von Software as a Service, die durch einen Cloud-Service-Provider in einem Rechenzentrum bereitgestellt wird.

Vorteile

- Die Wartung der Infrastruktur und der Software wird durch den Anbieter übernommen.
- Günstiger als der Aufbau und die Wartung einer Private-Cloud-Lösung.
- Das Know-how zum Schutz der Daten ist in einem zertifizierten Unternehmen sehr hoch einzuschätzen.

Nachteile

- Datenbanken können vom Cloud-Service-Provider eingesehen werden. Es besteht hierdurch die Gefahr des Verlustes der Datenhoheit (siehe Kapitel 2.1).
- Der Zugriff auf die Webschnittstelle ist öffentlich verfügbar und wird nur über die Passwortqualität der Nutzer geschützt.
- Unsicherheiten bei einer Insolvenz des Cloud-Service-Providers.

1.5.5 Private-Cloud ï Software as a Service

Im Folgenden werden grundlegende Vor- und Nachteile von Software as a Service im Bereich der Private-Cloud dargestellt.

Beispiel:
Ein Handwerksunternehmen hat einen eigenen Server auf dem Software für die Mitarbeiter bereitgestellt wird.

Vorteile

- Die Daten sind auf der eigenen Infrastruktur nicht durch Dritte einsehbar.
- Es können Software-Lösungen genutzt werden, die die Teamarbeitet im Unternehmen erhöhen kann.

Nachteile

- Hoher Aufwand: Es muss ein Server verfügbar sein, der im eigenen Unternehmen vorhanden ist und fachgerecht gewartet werden muss.
- Die Nachteile von IaaS in einer Private-Cloud sind vollständig auf SaaS in einer Private-Cloud übertragbar, (siehe Kapitel 0.)

1.5.6 Software as a Service ï Risiken

Der Aufwand für Handwerksunternehmen eine Private-Cloud zu errichten, die auf eigenen Servern betrieben wird, ist sehr hoch und die Umsetzung wenig realistisch. Die Gefahren durch falsche Konfigurationen oder mangelnde Updateroutinen können deutliche Risiken für die Unternehmensdaten mit sich bringen. In der Public-Cloud hingegen kann die Nutzung von SaaS durch Handwerksunternehmen oft einfacher und sicherer gestaltet werden, es bleiben dennoch Risiken bei der Verwendung von Cloud-Diensten, die in Kapitel 2 ausführlich dargestellt werden.

1.6 Verbreitung von Cloud-Computing im Handwerk

Cloud-Computing ist nicht nur für große Unternehmen ein spannendes Thema, auch für Handwerksunternehmen gibt es bereits Branchenlösungen, die im täglichen Gebrauch eingesetzt werden können (siehe Kapitel 4).

Aus der Studie (Stand der IT-Sicherheit im Handwerk, 2013) geht folgendes hervor*:*

Ă*Die bisher gering verbreitete Nutzung des Cloud-Computing im Handwerk wird durch die hier vorliegende Befragung unterstützt. Nur 10,2% der Betriebe geben an, von Cloud-Computing Technologien Gebrauch zu machen. Die Ergebnisse dieser Untersuchung zeigen ebenfalls, dass sich der derzeitige Nutzungsgrad des Cloud-Computings zwischen den Betriebsgrößenklassen kaum unterscheidet. Kleinstbetriebe mit weniger als fünf Mitarbeitern nutzen im Schnitt mit 16,5% am häufigsten eine Cloud. Betriebe mit fünf bis neun Mitarbeitern und die Betriebe mit zehn bis weniger als 20 Mitarbeitern verwenden in rund 14% der Fälle bereits die Möglichkeit des Cloud-Computings. Innerhalb der Betriebsgrößenklasse von 20 bis weniger als 50 Mitarbeiter geben 12,5% der Befragten an Daten in einer Cloud abzulegen.****ñ***

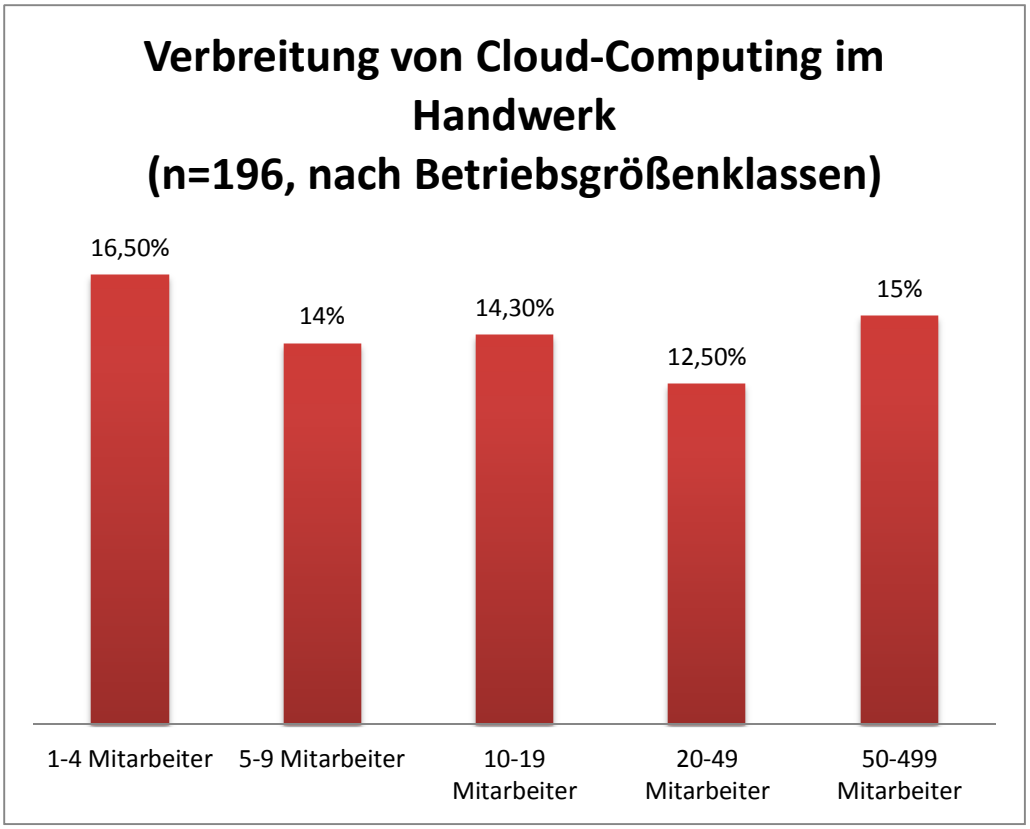


Abbildung 4: Verbreitung von Cloud-Computing im Handwerk

1.7 Vorteile von Cloud-Computing

In den folgenden Abschnitten werden die Vorteile von Cloud-Computing beschrieben, jedoch sollten Sie sich nicht verfrüht zum Einsatz von Cloud-Computing verleiten lassen. Ebenso sollten Sie sich auch mit Kapitel 1.8 (Nachteile von Cloud-Computing) und Kapitel 2 (Risiken bei der Nutzung von Cloud-Computing) befassen, in denen Risiken aufgeführt werden, die bei der Nutzung von Cloud-Computing entstehen können.

1.7.1 Kosten

Cloud-Computing kann kostengünstiger sein. Vergleichen Sie die Angebote dennoch mit üblichen Softwareangeboten.

Ein Synergie-Effekt beim Public-Cloud-Computing ist, dass Cloud-Service-Provider ihre Rechenzentren besser auslasten können, wenn ihre Dienste von vielen Kunden genutzt werden. Dies ermöglicht es den Anbietern, die Kosten pro Speicher- oder Recheneinheit für einen günstigeren Preis anbieten zu können.
Es bleibt aber zu bemerken, dass beim Beispiel Software as a Service nicht generell behauptet werden kann, dass Cloud-Computing immer die günstigere Alternative ist. Angebote aus dem Bereich Cloud-Computing sollten aus diesen Gründen immer mit alternativen und bewährten Softwareinstallationen verglichen werden.

1.7.2 Know-how in puncto IT-Sicherheit nutzen

Bei Cloud-Computing kann das Know-how von IT-Erfahrenen und kompetenten Unternehmen genutzt werden.

Wenn Cloud-Computing im Unternehmen eingesetzt wird, kann dies im Bereich der IT-Sicherheit durchaus einen Vorteil bieten. Wenn Daten bei erfahrenen Cloud-Service-Providern gespeichert werden, haben diese bessere und oft effektivere Maßnahmen zum Schutz der Daten als übliche Handwerksunternehmen.
Bei Cloud-Computing und der Nutzung von Diensten in einer Public-Cloud fällt der Wartungsaufwand für Handwerksunternehmen bei Hardware- und Softwarekomponenten am Server weg, denn es wird ein bereitgestellter Server eines Cloud-Service-Providers genutzt, auf dem die Software ständig aktualisiert wird. Nicht nur, dass Cloud-Anbieter häufig ausgefeilte Prozesse und Routinen zum Schutz der IT-Sicherheit nutzen, sie haben auch weitaus mehr Experten, die sich täglich mit dem Schutz der Systeme auseinandersetzen und diese vor Angriffen aus dem Internet rüsten.

Ein Cloud-Service-Provider mit gebündeltem Know-how bezüglich der IT-Sicherheit ist deutlich besser aufgestellt als ein kleines Handwerksunternehmen.

1.7.3 Bedarfsgerechter Einsatz

Der bedarfsgerechte Einsatz von Cloud-Computing ergibt sich aus dem Abonnement-Modell, das heißt Ressourcen und Nutzer-Accounts können monatlich hinzugefügt und wieder gekündigt werden.

Bei Cloud-Computing können Ressourcen monatlich hinzu- und abbestellt werden.

Stellen Sie sich vor, es muss ein größeres Projekt für ein Unternehmen bearbeitet werden. Für die Bearbeitung dieses Auftrags wird eine bestimmte Software benötigt, die bei einem Cloud-Service-Provider für eine gewisse Zeit gebucht werden kann. Nach Beendigung des Projektes werden die verwendeten Lizenzen abbestellt.

Der Vorteil, der sich hierbei ergibt, ist klar ersichtlich: Es musste keine Software für die Mitarbeiter bestellt werden, die diese nach einem Projektabschluss nicht mehr benötigen. Durch diesen bedarfsgerechten Einsatz von Cloud-Computing ist es möglich, die Kosten der einmaligen Anschaffung einer Software zu sparen und nur einen Bruchteil der eigentlichen Kosten zahlen zu müssen.

Bei Cloud-Computing können je nach Bedarf Rechenleistung oder zusätzliche Lizenzen für Nutzer hinzugebucht oder abbestellt werden.

1.7.4 Wartungsaufwand

Die Wartung der Serversysteme wird durch den Cloud-Computing-Dienstleister durchgeführt.

Die Wartung der Software in einer Public-Cloud wird durch den Cloud-Service-Provider übernommen, auch die Infrastruktur auf der die Software bereitgestellt wird, ist durch den Anbieter gleichermaßen abgedeckt.
Wenn jedoch virtuelle Maschinen im Bereich von Infrastructure as a Service genutzt werden, müssen Kunden selber für die Aktualität der einzelnen Betriebssysteme und Softwarekomponenten sorgen. Damit entsteht eine Pflicht, die durch den Kunden des Cloud-Services selbst übernommen werden muss. Durch diesen Einsatz von Cloud-Computing würde sich der Aufwand für die Wartung und das Risiko aufgrund nicht geschlossener Sicherheitslücken erhöhen.

1.7.5 Skalierbarkeit und Flexibilität

Durch die einfachen Managementoberflächen lassen sich nach Belieben Auslastungsspitzen abfangen, die beispielsweise durch hohe Nutzerzahlen oder einen höheren Rechenaufwand entstehen können. Dabei wird vom System erkannt, dass eine Auslastung über einen festgelegen Maximalwert steigt. Je nach Konfiguration startet an diesem Punkt eine automatische Skalierung der Ressourcen.

Cloud-Computing bietet hohe Skalierbarkeit und Flexibilität, Ressourcen können per Mausklick hinzugefügt werden.

Eine hohe Flexibilität kann durch das einfache Lizenzmodell bei Cloud-Computing erreicht werden, demnach müssen keine einmaligen und kostspieligen Lizenzen angeschafft werden. Ganz im Gegenteil, es können dann Software-Pakete gebucht werden, wenn sie durch einen Mitarbeiter Verwendung finden.

1.7.6 Hohe Verfügbarkeit

Cloud-Service-Provider bieten üblicherweise eine hohe garantierte Verfügbarkeit der Nutzerdaten an. Häufig wird in Angeboten damit geworben, dass eine Verfügbarkeit von 99,9% erreicht wird. Dies beutet, dass ein System das 24 Stunden am Tag, an 365 Jahrestagen läuft, maximal für 8,76 Stunden im Jahr ausfallen darf.

Einfache Redundanz kann durch das mehrfache Vorhandensein von Festplatten, so genannten RAID-Systemen, erreicht werden. Für höhere Verfügbarkeiten müssen auch größere Kosten in Kauf genommen werden, da ein Cloud-Service-Provider dies mit größerem Aufwand realisieren muss. Dies bedeutet die Anschaffung aller Komponenten in einem Rechenzentrum in mindestens zweifacher Ausführung, vom Notstromaggregat bis hin zu einem zweiten Anschluss an einen Internetprovider. Die höchste Redundanz kann durch geografisch unabhängige Rechenzentren erreicht werden. Dies schützt Daten insbesondere vor regionalen Katastrophen und daraus resultierenden Schäden durch Wasser, Feuer oder Erschütterungen.

Cloud-Computing bei professionellen Anbietern kann eine hohe Verfügbarkeit aufweisen.

1.8 Nachteile von Cloud-Computing

Nutzer sollten sich unter keinen Umständen durch günstige Konditionen verfrüht zur Verwendung von Cloud-Computing verleiten lassen.
Auch bei Cloud-Computing hat jeder Anwender und jedes Unternehmen eine rechtliche Verantwortung gegenüber den Daten und Informationen, die in die Cloud transportiert werden.

1.8.1 Abhängigkeit

Die Abhängigkeit im Bereich Cloud-Computing beschreibt ein Szenario, dass die Gefahr birgt, durch einen Cloud-Service-Provider an ein proprietäres und nicht offenes Format gebunden zu werden. Dieses Problem macht es für einen Kunden schwierig zu einem anderen Anbieter zu wechseln, da eine Verschiebung der Informationen zu einem hohen Aufwand bei einem Anbieterwechsel führt. Dies bezieht sich vor allem auf das Rückgabeformat der Daten bei der Vertragsbeendigung. Daher ist es bedeutend, vor einem Vertragsschluss das Rückgabeformat festzulegen.

Abhängigkeit beschreibt die Gefahr, wenn Cloud-Dienste genutzt werden, die kein standardisiertes Rückgabeformat nach Vertragsbeendigung anbieten.

Prüfen Sie vor einem Vertragsabschluss, wie das Rückgabeformat der Daten nach einer möglichen Vertragsbeendigung geregelt ist. Das Format sollte gängigen Standards entsprechen, zum Beispiel SQL[2] oder MySQL[3].

1.8.2 Netzzugang und Arbeitsgeschwindigkeit

Für Cloud-Computing ist ein schneller Internetanschuss Voraussetzung. Dies sollte je nach Nutzeranzahl mindestens ein DSL-Anschluss sein.

Da Cloud-Computing mit den Ressourcen eines Cloud-Service-Providers ausgeführt wird, sollte ein konstanter und schneller Netzzugang vorhanden sein. In ländlichen Gebieten sind häufig noch keine schnellen Internetzugänge verfügbar. Aus diesem Grund ist es wichtig, dass die Bandbreite vor der Nutzung von Cloud-Computing bestimmt wird. Ist die Bandbreite nicht für Cloud-Computing geeignet, sollte ein schnellerer Netzzugang angefordert werden. Da gerade in ländlichen Regionen häufig nur langsame Internetanbindungen angeboten werden, ist es ratsam sich von dem Cloud-Anbieter über die bestehende Internetanbindung beraten zu lassen. In Kapitel 4.2 werden einige Mindestanforderungen dargestellt. Es wird aber generell ein DSL-Anschluss mit mindestens 1000 kbit/s empfohlen. Beachten Sie darüber hinaus, dass mit mehr Arbeitsplätzen auch die notwendige Bandbreite erhöht werden muss.

Einen Bandbreitentest können Sie beispielsweise auf der Internetseite http://dsl-speedtest.computerbild.de durchführen.
Der Netzzugang des Handwerksunternehmens sollte stabil und schnell genug sein, um eine komfortable Nutzung von Cloud-Diensten zu ermöglichen.

1.8.3 Funktionsumfang

Der Funktionsumfang von Cloud-Systemen muss vertraglich vereinbart werden.

Die Bedeutung des Funktionsumfangs lässt sich an folgendem Beispiel veranschaulichen:
In der Ausgangssituation wird eine Software aus der Cloud verwendet. Prozesse und Arbeitsabläufe im Unternehmen wurden auf diese Software optimiert. Nun entscheidet sich der Cloud-Service-Provider dazu, die genutzte Anwendung zu verändern. Dies hat zur Folge, dass alle Arbeitsabläufe im eigenen Unternehmen geändert und ebenfalls angepasst werden müssen.
Der Kunde von Software as a Service hat möglicherweise kein Mitspracherecht, wenn sich ein Cloud-Anbieter dazu entschließt, bestimmte Funktionalitäten zu ändern oder gegebenenfalls nur noch gegen einen Aufpreis anzubieten.
Ein weiteres Szenario wäre, dass ein Cloud-Service-Provider eine Software nicht weiter pflegt und die Serviceverträge auslaufen lässt. Dies könnte bedeuten, dass Kunden zum Wechsel zu aktuelleren Anwendungen gezwungen werden.

Der Funktionsumfang und Unterstützung der Dienste sollte im Service-Level-Agreement festgehalten werden.

---

[2] *SQL ï Structured Query Language ist eine standardisierte Datenbanksprache*
[3] *MySQL ï Weit verbreitete, relationale Datenbanksprache*

1.8.4 Verlässlichkeit

Durch Sicherheitsvorfälle in der Vergangenheit kam es wiederholt zu Ausfällen bei verschiedenen Anbietern. In Folge dessen hatten Kunden von Cloud-Services keinen Zugriff auf ihre Daten.
Ein Szenario mit weitaus gravierenderen Folgen wäre ein Ausfall bei einem Cloud-Service-Provider mit zusätzlichem Datenverlust. Wenn in diesem Fall keine Backups der Daten im eigenen Unternehmen erstellt wurden, sind diese unwiederbringlich verloren.

Auch Cloud-Service-Provider können von massiven Ausfällen bis hin zum Datenverlust betroffen sein.

Zu einem gravierenden Vorfall ist es 2009 bei Kunden von T-Mobile gekommen (Andreas Wilkens, 2009), die das Mobiltelefon vom Typ Sidekick nutzten. Bei dieser Art von Smartphone wurden viele persönliche Daten wie beispielsweise Telefonbuch, Kalenderdaten und Bilder ausschließlich in der Cloud, also auf Serversystemen bei einem Microsoft Tochterunternehmen mit dem Namen Danger abgespeichert. Auf Grund unzureichender Backup-Funktionalitäten, die aus Kostengründen eingespart wurden, ist es nach einem Server-Fehler zu diesem Ausfall gekommen (Matt Hickey, Stefan Beiersmann, 2009). Bei einigen Nutzern ist es zu einem vollständigen Datenverlust gekommen.

Bei Cloud-Computing und ebenso bei anderen Dienstleitern sind Kunden demnach immer abhängig von der Verlässlichkeit der einzelnen Services und Dienstleister. Dies muss Nutzern von Cloud-Diensten bewusst sein. Die Verlässlichkeit der einzelnen Dienste muss deshalb in einem Service Level Agreement zwischen Anbieter und Kunden vertraglich geregelt werden, um nach Vertragsbrüchen rechtlich gegen diese vorgehen und möglichen Schadensersatz einfordern zu können.

Prüfen Sie die Verfügbarkeit von Anbietern, durch eine Suche in bekannten Suchmaschinen, auf bekannt gewordene Ausfälle und achten Sie darauf, dass eine Verfügbarkeit von mindestens 99.9% auf ein Jahr hin angeboten wird.

1.8.5 Skalierung und mögliche Folgen

Für den Einsatz von automatischer Skalierung, also einem automatisierten Erhöhen der Ressourcen bei einer Überlastung, sind besondere Sicherheitsvorkehrungen zu treffen. Hierbei sollte bedacht werden, dass dieses Verhalten auch durch Schadsoftware oder durch unbekannte Dritte hervorgerufen werden kann.
Diese müssten sich zwar Zugang zur Administrationsoberfläche verschaffen aber die Möglichkeit, dass ein Administrator auf einen Phishing-Angriff herein fällt oder durch einen Trojaner belauscht wird, kann nicht ausgeschlossen werden. Dies würde einen Angreifer in den Besitz von Zugangsdaten bringen, die er gegen ein Unternehmen oder gar mehrere Unternehmen nutzen kann.
Daher sollte unbedingt der Administrator automatisch über eine Skalierung informiert werden, dies kann beispielsweise per SMS oder E-Mail passieren. Im Fall einer schadhaften Ursache müsste sofort reagiert werden, indem der Cloud-Service-Provider über diesen Vorfall informiert wird. Falls ein Account gehackt wurde, muss dieser sofort gesperrt werden.

Bei einem Phishing-Angriff wird versucht, ein Opfer zur Eingabe von Nutzerinformationen wie Passwort und Benutzername zu verleiten.

Wird bei Cloud-Computing die Möglichkeit von automatischen Skalierungen hinsichtlich der Systemleistung verwendet, sollte der Verantwortliche über eine Ressourcenbuchung automatisch informiert werden.

1.9 Zusammenfassung

In diesem Kapitel wurden grundlegende Zusammenhänge für ein Basiswissen im Bereich Cloud-Computing dargestellt. Mit der Erörterung von Vor- und Nachteilen sind Sie gerüstet, um Mitarbeitern in einem Unternehmen klar zu machen, welche Probleme oder welchen Gewinn die Nutzung von Cloud-Computing mit sich bringen kann. Darüber hinaus wurden einige Tipps gegeben, wie Probleme im Grundsatz vermieden werden können.

2. Risiken bei der Nutzung von Cloud-Computing

Wie bei jeder Infrastruktur, Plattform oder Software gibt es auch beim Cloud-Computing Risiken, die vor der Verwendung eines Cloud-Dienstes bedacht werden müssen. Auch Restrisiken wie eine Insolvenz (siehe Kapitel 2.3.2) eines Cloud-Service-Providers können nicht vollständig ausgeschlossen werden.

2.1 Möglicher Verlust der Datenhoheit[4]

Wird ein Public-Cloud-Dienst genutzt um Informationen zu speichern (Storage as a Service), besteht die Möglichkeit, Daten vor dem Versand in die Cloud zu verschlüsseln. Der Anbieter einer Cloud ist somit nicht in der Lage, die Daten ohne den Schlüssel des Nutzers zu entschlüsseln.

Der Verlust der Datenhoheit beschreibt das Problem, wenn Firmengeheimnisse an einen Cloud-Service-Provider ausgelagert werden und diese auf Grund fehlender Verschlüsselungen vom Anbieter eingesehen werden können.

Bei Software as a Service ist dies anders. Werden auf Datenportalen zum Beispiel E-Mails oder ganze Kundenverwaltungssysteme abgelegt, sind diese für den Cloud-Anbieter unmittelbar einsehbar, die Datenhoheit, also die volle Kontrolle und der Zugriffsschutz vor Dritten ist demnach gefährdet. Der Grund dafür ist, dass durch Datenbankabfragen die Logik der Software auf dem Server des Cloud-Anbieters im Besitz des Schlüssels sein muss, insbesondere wenn dieser verschlüsselt ist. Das bedeutet, dass ein privater Schlüssel auf dem Server des Cloud-Service-Providers angelegt und verwaltet werden muss.
Dies hat zur Folge, dass der Dienstanbieter auf die Daten zugreifen könnte. Dieser Nachteil beschreibt allgemein die Problematik für einen möglichen Verlust der Datenhoheit. Firmenkritische Informationen könnten so von Insidern oder unbekannten Dritten mitgelesen werden, insbesondere in Staaten, in denen ein deutsches Datenschutzniveau fehlt.

2.2 Unternehmerischer Datenmissbrauch

Wenn Daten in die Cloud verschoben werden, muss das Risiko eingegangen werden, dass auch Dritte Einsicht in diese Daten haben können. Dies gilt insbesondere bei der Verwendung von Software as a Service, wie zuvor beschrieben.
Falls trotz aller Sicherheitsmaßnahmen ein Vorfall bezüglich mangelnder IT-Sicherheit bei einem Cloud-Service-Provider eintritt, könnten sich auch Angreifer dieser Möglichkeit bedienen und Daten abgreifen. Diese Problematik gefährdet nicht nur die gespeicherten Informationen, ein möglicher Datenverlust oder -missbrauch ist sogar meldepflichtig, wenn in größerem Umfang Nutzer oder Kundendaten gestohlen wurden. Diese Pflicht ist durch § 42a des Bundesdatenschutzgesetzes (BDSG) gesetzlich verankert.
Eine andere Gefahrenlage könnte beispielsweise entstehen, wenn Infrastructure as a Service genutzt wird und eine dynamische Hinzubuchung von Ressourcen ausgeführt

Ein Brute-Force-Angriff ist eine Methode, bei der zufällig generierte Passwörter oder Wörter aus Wortlisten gegen ein Login-Portal verwendet werden, um Zugriff zu erlangen.

[4] *Datenhoheit, beschreibt das Zugriffsrecht durch ein einzelnes Unternehmen. Ein Zugriff durch Dritte und ein Zugriff durch einen CSP bleiben verwehrt.*

wird. Diese Rechenleistung rückt in den Fokus von Angreifern. Diese könnten versuchen, über den Einsatz von Phishing oder mit purer Gewalt über einen Brute-Force-Angriff auf ein Login-Portal in den Besitz von Administrationsrechten zu gelangen, um diese Infrastruktur in ihren Besitzt zu bringen. Es wäre so möglich, neue virtuelle Maschinen hinzu zu buchen, ohne dass der eigentliche Nutzer etwas davon erfährt. Der Nutzer würde von dem Missbrauch erst im Rahmen von späteren Ermittlungen erfahren.

2.2.1 Viren und Schadsoftware in der Cloud

Anbieter von Cloud-Services müssen geeignete Strategien gegen Viren und Schadsoftware in der Cloud verwenden, beispielsweise IDS-/IPS-Systeme.
Aus strategischen Gründen werden genaue technische Details häufig geheim gehalten.

Viren und Schadsoftware sind nicht nur Risikofaktoren für Nutzer und Unternehmen ansich, sie gefährden ebenso gesamte Cloud-Systeme. Unterschiede zeigen sich aber hinsichtlich der Abwehrmaßnahmen. Ein Handwerksunternehmen verwendet typischerweise eine Antivirensoftware um einen Basisschutz zu gewährleisten. Cloud-Service-Provider hingegen setzen auf weitaus fortschrittlichere Methoden, um schadhaften Netzwerkverkehr oder Angriffe zu erkennen und zu bekämpfen. Dazu zählen Technologien wie Intrusion Detection Systems (IDS, zu Deutsch Angriffserkennung) und Intrusion Prevention Systems (IPS, zu Deutsch Angriffsvermeidung), um sich gegen Angriffe von außen sowie vor der Kommunikation von Schadsoftware mittels signaturbasierter Datenanalyse zu schützen. Diese Technologien können auf der Grundlage von Signaturen Schadcode im Datenstrom eines Rechenzentrums identifizieren und abwehren.

Informieren Sie sich darüber, ob ein Anbieter IDS- und IPS-Systeme zum Schutz vor Angriffen aus dem Internet verwendet.

2.2.2 Hacken und Cloud

Verschiedene Ereignisse haben aufgezeigt, dass Cloud-Service-Provider im Bereich Software as a Service Ziel von Hackern wurden:

- Spam-Wellen nach Angriff auf Administrator bei Dropbox[5] (Björn Greif, 2013)
- Hack des Dienstes Evernote[6] (Ronald Eickenberg, 2013)

Anbieter von Cloud-Services wurden in der Vergangenheit immer wieder Ziel von Hackerangriffen.

Stellen Sie sich vor, einem Angreifer würde die Übernahme von Ressourcen eines der großen Cloud-Service-Provider gelingen. Dieses Szenario hätte zur Folge, dass nicht nur Nutzer von so einem Angriff betroffen wären, auch das Ausmaß von Folgeangriffen mit diesen gehackten Kapazitäten wäre kaum auszudenken. Es könnte ebenso zu Attacken auf Infrastrukturen oder andere Dienstleister führen.
Daher ist essentiell, dass sich auch die Sicherheitsvorkehrungen der verschiedenen Cloud-Service-Provider auf einem sehr hohen Niveau befinden. Dieses Niveau lässt sich aus der Bereitschaft zu Zertifizierungen ableiten (siehe Kapitel 4.3.2).

Zertifizierungen sind ein Erkennungsmerkmal für geprüfte und sichere Unternehmens-Strukturen. Wählen Sie zertifizierte Cloud-Service-Provider aus.

[5] *Dropbox ï US-Unternehmen mit Fokus auf Online-Datenspeicher*
[6] *Evernote ï US-Unternehmen mit Cloud-Dienst für Notizen*

Bei dem Thema Hacken und Cloud darf nicht außer Acht gelassen werden, dass Hacker zukünftig auch Zugriff auf das Potenzial von Cloud-Computing haben und diese nutzen können, um illegale Aktivitäten auszuführen. Solche Aktivitäten könnten unter anderem das Ausführen von DDoS-Angriff[7] (siehe Handbuch Netzwerksicherheit) auf andere Nutzer oder das Errechnen von Schlüsseln aus erbeuteten Datenbankinformationen sein. Für diese illegalen Aktivitäten werden kurzfristig angemietete Infrastrukturen genutzt, um hoch rechenintensive Aufgaben zu erfüllen oder um große Bandbreiten zu nutzen.

2.3 Kritische Handlungsfelder in der Cloud

In diesem Unterkapitel werden kritische Handlungsfelder dargestellt, welche die Verfügbarkeit der Cloud-Dienste einschränken oder durch einen Totalausfall völlig zum Erliegen bringen können.

2.3.1 Verlust der Verfügbarkeit bei Totalausfällen

Beispiele aus der Vergangenheit haben gezeigt, dass nicht nur kleine Cloud-Service-Provider von mehrtägigen Ausfällen betroffen sein können, auch große Anbieter von Cloud-Services sind bei Zwischenfällen in Bedrängnis geraten (s. Kapitel 1.8.4).
Ein solcher Ausfall hat multiple Folgen, beispielsweise die Nichterreichbarkeit der Dienste, bis hin zu einem Teilverlust der Daten, schlimmstenfalls können Daten nicht wiederhergestellt werden. Zusätzlich sollte die Möglichkeit eines manuellen Backups auf der lokalen Infrastruktur genutzt werden, alternativ eine Backupfunktion auf der redundanten Infrastruktur des CSP, wenn die Funktionalität des Cloud-Dienstes dieses anbietet.

Lokale Backups können Sie vor Datenverlust, jedoch nicht vor Problemen bei der Verfügbarkeit einzelner Dienste schützen.

2.3.2 Insolvenz eines Cloud-Anbieters

Ein mögliches Risiko bei der Nutzung von Cloud-Diensten ist die Insolvenz eines Cloud-Service-Providers. Dabei muss ausdrücklich darauf verwiesen werden, dass ein direktes Vertragsverhältnis zwischen einem Cloud-Service-Provider und einem Kunden nicht angetastet wird.
Im schlimmsten Fall ist es möglich, den Insolvenzverwalter zur Herausgabe der Daten zu bewegen, da ein Recht auf Aussonderung besteht.

[7] *DDoS ï Distributed Denial of Service, ein Angriff der mit einer hohen Datenflut gezielt die Nichtverfügbarkeit von Web-Diensten erreichen kann*

Die Insolvenz eines Unternehmens in Deutschland ist gesetzlich geregelt. Sie haben ein Recht auf die Herausgabe von Daten.

Insolvenzverordnung § 47 Aussonderung:
ĂWer auf Grund eines dinglichen oder persönlichen Rechts geltend machen kann, dass ein Gegenstand nicht zur Insolvenzmasse gehört, ist kein Insolvenzgläubiger. Sein Anspruch auf Aussonderung des Gegenstands bestimmt sich nach den Gesetzen, die außerhalb des Insolvenzverfahrens gelten.ñ[8]

Sitzt ein Cloud-Service-Provider im Ausland, ist das geltende Recht des jeweiligen Landes zu berücksichtigen, ebenso bei Ländern aus dem Europäischen Wirtschaftsraum.

Regeln Sie vor der Vertragsschließung mit einem Cloud-Service-Provider, wie im Fall einer Insolvenz weiter vorgegangen wird. Es sollte vertraglich geregelt werden, dass der Zugriff auf Daten auch nach einer Insolvenz gewährleistet wird.

2.3.3 Vendor Lock-in (Anbieterabhängigkeit)

Geeignete und standardisierte Rückgabeformate in Form von beispielsweise SQL, sollten vor einem Vertragsabschluss berücksichtigt werden.

Wenn ein Kunde eines Cloud-Service-Providers unachtsam bei der Auswahl der genutzten Dienste war, kann es passieren, dass dieser in eine Abhängigkeit gerät. Ein Anbieterwechsel in einer solchen Situation kann sehr aufwändig und teuer werden.

Eine Mutwilligkeit seitens der Service-Anbieter soll hier nicht unterstellt werden, allerdings ist die Möglichkeit gegeben, offene Standards für die Portierung zu anderen Anbietern bereit zu stellen.

Achten Sie bei der Auswahl eines Cloud-Service-Providers auf das Rückgabeformat bei der Beendigung der Vertragsverhältnisse.

2.4 Zusammenfassung

Es ist zusammenfassend darzustellen, dass viele kritische Handlungsfelder in Cloud-Computing im Voraus vertraglich abgesichert werden können. Kommt es jedoch zu Problemen bei der Verfügbarkeit, sind finanzielle Schäden für ein Handwerksunternehmen nicht auszuschließen. Einen großen Schutz bieten daher lokale Daten-Backups, um im Notfall ein Aufrechthalten der Verwaltung gewährleisten zu können.

[8] *http://dejure.org/gesetze/InsO/47.html ï Insolvenzverordnung § 47 Aussonderung*

3. Basisschutz: Handlungsempfehlungen

Bei Cloud-Computing ist ein adäquater Basisschutz auf allen verwendeten Geräten unerlässlich.
Wichtige Schutzkomponenten wie Antivirensoftware und eine Firewall sollten auf jedem Computer installiert sein. Zu den Software-Lösungen gehört auch ein gewisses Maß an Achtsamkeit. Dabei sollte einem Anwender vor dem Ausführen einer Installation oder dem Öffnen von E-Mail-Anhängen bei unbekannten oder gefälschten Absendern immer bewusst sein, dass diese Daten auch mit schadhaften Inhalten belastet sein könnten.
Bei Cloud-Computing besteht die Möglichkeit, von verschiedenen Geräten, wie beispielsweise Smartphone oder Laptops, auf eine Cloud-Umgebung zugreifen zu können. Dies öffnet für unbekannte Dritte Tür und Tor für das Mitlesen von Passwörtern auf manipulierten Geräten.
Eine Möglichkeit besteht darin, den Zugriff auf Cloud-Lösungen nur von bestimmten Adressräumen zu erlauben, also beispielsweise nur aus dem Firmennetzwerk oder über eine Verbindung vom Firmenlaptop über einen VPN-Zugang.

3.1 Basisschutz auf Geräten

Ein unumgänglicher und wichtiger Punkt ist ein effektiver Basisschutz auf allen für Cloud-Computing eingesetzten Geräten. Ob es nun Smartphones, Tablets oder Computer sind, spielt keine große Rolle, ein grundlegender Schutz dieser Geräte ist von absoluter Wichtigkeit.

3.1.1 Updates

Eine Vielzahl von Geräten bringt auch eine hohe Anzahl von potenziellen Sicherheitslücken mit sich, diese gilt es, mit von Herstellern herausgegeben Updates, zu schließen. Hierbei können auch Sicherheits-Suiten helfen, die Sie vor veralteten Programmen warnen oder zum Update Ihres Betriebssystems auffordern.

Security-Suiten können Ihnen helfen, Ihr System und Ihre Software aktuell zu halten.

Achten Sie daher immer darauf, dass die automatischen Updateroutinen des jeweiligen Gerätes aktiviert sind.

3.1.2 Sichere Passwörter

Die Wahl von starken Passwörtern ist ein Sicherheitsmerkmal, welches potenziellen Angreifern den Zugriff auf ein System verwehrt. Hacker haben die Möglichkeit, einen so genannten Brute-Force-Angriff auf ein Login eines Nutzers auszuführen. Wenn diese Attacke nicht frühzeitig erkannt wird und der Nutzer ein schlechtes Passwort gewählt hat, kann mit Begrifflichkeiten aus einer umfangreichen Wortliste das Nutzerkennwort erraten werden.

Nutzen Sie sichere Passwörter mit folgenden Kriterien!

Bei der Auswahl von Passwörtern sind folgende Punkte zu beachten:

- Verwenden Sie mindestens zehn Zeichen, darunter eine Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen in sinnfreiem Zusammenhang.
- Ändern Sie Passwörter regelmäßig.
- Nutzen Sie für jedes Login ein separates Kennwort.
- Bewahren Sie Ihre Passwörter sicher auf. Hierzu eignen sich Passwort-Management-Programme wie keePass(x)[9].

Passwortverwaltungssoftware wie keePass(x) können helfen, Kennwörter sicherer zu Verwalten.

Was unbedingt vermieden werden sollte:

- Nutzen Sie keine zusammenhängenden Wörter, die im Lexikon oder im allgemeinen Sprachgebrauch vorkommen (schlechtes Beispiel: Jahreszeiten, Lieblingsverein, Name).
- Nutzen Sie keine Begriffe, die mit Ihnen in Bezug gebracht werden können ï wie den Namen eines Familienmitglieds oder Ihres Lieblingssportvereins.
- Hängen Sie keine Jahreszahlen oder Geburtstage an Kennwörter.

3.1.3 Security-Suiten

Ein Phishing-Angriff wird häufig durch eine fingierte E-Mail initiiert. Diese enthält einen Link, der auf eine präparierte Seite verweist, wo ein potenzielles Opfer über das Ausnutzen von Sicherheitslücken mit Schadsoftware infiziert werden kann.

Damit beispielsweise Schädlinge in E-Mails oder auf USB-Sticks erkannt werden können, ist es notwendig eine aktuelle Sicherheitssoftware auf allen verwendeten Geräten zu installieren.
Dabei sollte nach Möglichkeit eine Software verwendet werden, die gleichermaßen eine Antivirenlösung und eine Firewall beinhaltet. Werden beide Lösungen aus einer Hand angeboten ist auch die Pflege der Software einfacher.
In einem Handwerksunternehmen sollte sich daher auf eine einzelne Security-Suite geeinigt werden um den Wartungsaufwand und die Lizenzverwaltung möglichst gering zu halten.
Eine wichtige Funktion einer Sicherheitssoftware sollte auch das überprüfen von E-Mails auf mögliche Phishing-Angriffe sein.

Nutzen Sie eine umfangreiche und gute Security-Suite und achten Sie auf folgende wichtige Komponenten:

- Firewall-Funktionalität zum Schutz vor Angreifern aus dem Netzwerk.
- Antivirenlösung zum Erkennen von Schädlingen in E-Mails.
- Schutz vor Phishing- und Spam-Mails.
- Scan von heruntergeladenen Dateien.
- Dateisystemschutz durch geplante Scans in wöchentlichen Intervallen.
- Schutz vor schadhaften Webseiten.
- Warnfunktion zum Schutz vor veralteter Software.

[9] http://keepass.info ï *Kostenloser und quelloffener Passwortmanager*

3.2 Zugriff auf Cloud-Ressourcen

Der Zugriff auf Cloud-Ressourcen kann auf zwei verschiedene Art und Weisen realisiert werden.
Die eine Möglichkeit basiert auf dem Zugriff über eine Internetseite. Auf dieser Seite muss der Nutzer seine Zugangsdaten wie Nutzernamen oder E-Mail-Adresse eingeben, zusätzlich wird ein Kennwort verlangt.
Die andere Möglichkeit wird über ein Programm realisiert, welches lokal auf dem Computer oder Smartphone des Anwenders installiert wird.
Bei der Erstinstallation werden auch hier die Nutzerinformationen (Nutzername und Passwort) benötigt. Es ist davon abzuraten, Passwörter durch eine Applikation oder im Browser zu speichern. Diese Funktion hat den Nachteil, dass ein Passwort auf dem System hinterlegt wird. Besser ist es bei einem Neustart des Programms jeweils die Nutzerinformationen erneut einzugeben, auch wenn dies einen Aufwand für den Nutzer darstellt, ist es doch ein Zugewinn an Sicherheit.

Ein Verzicht auf Bequemlichkeit bringt häufig mehr Sicherheit mit sich.

3.2.1 Verschlüsselungstechniken bei der Datenübertragung

In diesem Abschnitt wird näher auf mögliche Zugriffsszenarien und Kanäle zur sicheren Datenübertragung eingegangen. Diese Methoden erlauben es, Informationen mit einer Ende-zu-Ende-Verschlüsselung bis zum Cloud-Service-Provider zu übertragen. Dritte haben hierbei nicht die Möglichkeit, diese Daten zu manipulieren oder zu entschlüsseln. Die folgenden Mechanismen sind Stand der Technik und sollten in einer dieser Formen zum Basisangebot eines jeden Cloud-Service-Providers gehören.

Die Übertragungsverschlüsselung ist von besonderer Bedeutung, sie ist ein effektiver und einfacher Weg, um Ihre Daten vor dem Zugriff durch Dritte zu schützen.

HTTPS

Bei der Nutzung eines Cloud-Dienstes sollten Sie stets sicherstellen, dass Sie eine SSL[10]/TLS[11]-geschützte Verbindung mittels HTTPS verwenden. Allgemein ist die Verwendung von Übertragungsverschlüsselungen ein gängiger Standard, den jeder Cloud-Service-Provider anbieten sollte. Der Dienst eines Cloud-Service-Providers sollte Sie beim Zugriff über den Browser direkt auf eine HTTPS-geschützte Seite weiterleiten, falls Sie aus Versehen in der Adresszeile des Internet-Browsers die http-Adresse eingegeben haben.
Falls keine HTTPS-Verschlüsselung zur Verfügung steht, ist dies ein Indiz für die mindere Qualität des Cloud-Anbieters.

Nutzen Sie nur verschlüsselte Verbindungen, um auf Daten bei einem Cloud-Anbieter zu-zugreifen bspw. SSL/TLS- oder VPN-geschützte Verbindungen.

[10] *SSL ï Secure Sockets Layer, Bezeichnung für ein Protokoll zur verschlüsselten Dateiübertragung*
[11] *TLS ï Transport Layer Security, hybrides Verschlüsselungsprotokoll, wird bei HTTPS verwendet*

VPN

Das Virtual Private Network (VPN) ist eine Möglichkeit, die Cloud-Service-Provider anbieten, damit sich ein Unternehmen verschlüsselt bis in die Infrastruktur des Cloud-Dienstes einwählen kann. Für diese Technik sollte der Cloud-Service-Provider eine Software bereitstellen, mit der die Verwaltung der Zertifikate und der Aufbau der Verbindung realisiert werden. Windows-basierte Computer haben eine eigene Softwarelösung von Microsoft an Board, häufig werden aber auch Lösungen über OpenVPN angeboten, die mit dem OpenVPN-Client[12] genutzt werden können. Beide Lösungen sind frei nutzbar. Ein anderer Softwareanbieter ist Cisco mit seinem Cisco AnyConnect[13], bei dieser Software gelten Lizenzbedingungen für den kommerziellen Einsatz.

Nutzen Sie die volle Bandbreite der bereitgestellten Sicherheitsmechanismen wie beispielsweise VPN oder SSL/TLS, um bei der Übertragung von Daten gegen die Einsicht und Manipulation durch Dritte geschützt zu sein.
Sorgen Sie für das Vorhandensein und die Aktualität einer Sicherheitssoftware mit Firewall- und Antivirenfunktionalität.

3.2.2 Zugriff von mobilen Geräten (BYOD)

Der Zugriff von mobilen Geräten, also beispielsweise Smartphones oder Tablets, kann durch eine vom Cloud-Service-Provider bereitgestellte App oder durch den Browser auf dem Gerät durchgeführt werden.
Wird der Zugriff durch einen Browser durchgeführt, ist wie bereits erwähnt auf die Verwendung einer HTTPS-geschützen Verbindung zu achten. Wenn eine App verwendet wird, muss durch den Anbieter sichergestellt sein, dass diese App nur über eine verschlüsselte Verbindung mit dem Cloud-Dienst kommuniziert. Der Kunde sollte sich die Verfügbarkeit von Verschlüsselungen durch den Anbieter bestätigen lassen. Dies kann auch in einem Service-Level-Agreement festgehalten werden.

Weitere Informationen zum Thema BYOD können Sie dem Handbuch ĂMobiles Arbeiten & Bring your own deviceñ entnehmen.

3.2.3 Verschlüsselung

Die Verschlüsselung im Bereich von Cloud-Computing ist ein vielfach diskutiertes Thema. Können dem Cloud-Service-Provider sensible Daten anvertraut werden oder sollten diese vor dem Hochladen in die Cloud vom Anwender verschlüsselt werden? Wo sind hier die Grenzen des technisch Möglichen?
Bei der Nutzung von Software as a Service bei einem externen Dienstleister kommt es zu einen unumgänglichen Problem: Werden Daten in eine verschlüsselte Datenbank bei einem Cloud-Service-Provider geschrieben, muss dieser im Besitz des privaten

[12] OpenVPN-Client http://openvpn.net/index.php/download/community-downloads.html
[13] Cisco AnyConnect http://www.cisco.com/c/en/us/solutions/enterprise-networks/anyconnect-secure-mobility-solution/index.html

Schlüssels sein. Dies ermöglicht dem Dienstanbieter einen Vollzugriff auf alle Informationen, die in der Datenbank gespeichert werden.
Hier besteht die bessere Alternative darin, Daten in einer Private-Cloud Struktur zu speichern.

Ruhende Daten

Ruhende Daten sind Informationen, die gespeichert und nicht dauerhaft verändert werden. Sie stehen im Gegensatz zu Datenbanken, die in ständiger Bearbeitung sind. Es bietet sich demnach an, Daten vor dem Speichern in der Cloud zu verschlüsseln. Dies hat den Vorteil, dass ein Cloud-Service-Provider nicht die Möglichkeit hat, auf diese Daten zuzugreifen, da nur der Urheber der Daten im Besitz des privaten Schlüssels ist. Diese Möglichkeit ist jedoch nur für Storage as a Service geeignet und dies auch nur bedingt. Wenn mehrere Nutzer an einem Dokument arbeiten müssen, wird eine Verschlüsselung schwierig. Dies kann beispielsweise der Fall sein, wenn ein Kollaborations-Tool zur Bearbeitung von Dokumenten in der Cloud verwendet wird.

Bei Storage as a Service, also dem Ablegen von Dateien in der Cloud, muss dies vom Nutzer selbst gelöst werden. Verschlüsseln Sie die Daten vor dem Hochladen in die Cloud lokal. Hierzu eignet sich beispielsweise das Programm TrueCrypt[14].

Daten in Bewegung

Daten in Bewegung beschreiben Dateien, die in ständiger Bearbeitung sind. Dies könnten ganze Datenbanken oder Dokumente sein, die von mehreren Nutzern gleichzeitig bearbeitet und verändert werden. Wie bereits beschrieben, kann und sollte ein Zugriff auf Datenbanken bei Cloud-Service-Providern verschlüsselt mittels VPN oder SSL erfolgen. Befinden sich diese Daten in einer unverschlüsselten Datenbank, so kann nicht gewährleistet werden, dass die Daten vor dem Zugriff durch den Cloud-Service-Provider selbst geschützt werden können.

Bei SaaS kann ein möglicher Zugriff auf die Daten durch einen Administrator bei Cloud-Service-Provider nicht ausgeschlossen werden.

Verschlüsselter Zugriff

Ein verschlüsselter Zugriff zum Schutz übertragener Daten vor der Einsicht Dritter kann über die bereits dargestellten Mechanismen, zum Beispiel per HTTPS oder VPN, gewährleistet werden.
Dies bedeutet jedoch, dass ausschließlich der Übertragungsweg verschlüsselt wird. Somit werden Daten auf einem Server nicht automatisch mitverschlüsselt. Diese Art von Verschlüsslung benötigt zusätzlich eine Dateiverschlüsselung.

[14] http://www.truecrypt.org ï *Freie Software zum Verschlüsseln von Festplatten und Datei-Containern*

3.2.4 Benutzergruppen-Management inkl. Rechte-Management

Viele Cloud-Computing Anbieter stellen die Möglichkeit bereit, die Rechte der Nutzer komfortabel auf einer Administrationsoberfläche zu verwalten.
Auf dieser Oberfläche kann der ausgewählte Administrator Nutzer hinzufügen und wieder löschen, darüber hinaus können beispielsweise der verwendete Speicherplatz und mögliche Rechte zum Teilen der Inhalte festgelegt werden.

Sind Benutzer- und Rechtemanagement in einer Cloud-Anwendung nötig, muss ein IT-erfahrener Mitarbeiter die Administration übernehmen.

Abbildung 5: Rechte-Management bei Owncloud[15]

Ein Administrator muss sich hier über seine Pflichten bewusst sein, denn die Verantwortung liegt darin, dass Nutzer korrekt authentifiziert werden, bevor für sie ein Account erstellt wird.

3.3 Zusammenfassung

Ein guter Basisschutz ist auch im Zeitalter des Cloud-Computings unerlässlich. Dies bedeutet, dass auf allen verwendeten Geräten geprüft werden muss, ob sich installierte Software und Betriebssysteme auf einem aktuellen Stand befinden. Auch die Passwortqualität spielt eine bedeutende Rolle. Schwache Passwörter machen es Angreifern leicht, mit Kenntnis eines Nutzernamens oder einer E-Mail-Adresse auf ein Webportal eines Cloud-Anbieters zuzugreifen.

[15] http://owncloud.org/ *Software, mit der Daten in einer Private-Cloud selbst verwaltet werden können.*

4. Cloud-Computing im Handwerk

In diesem Kapitel werden Anwendungsmöglichkeiten, ein beispielhaftes Szenario und eine Zusammenfassung der wichtigsten Kriterien bei der Nutzung von Cloud-Anwendungen dargestellt.

4.1 Anwendungsmöglichkeiten einer Cloud im Handwerksbetrieb

Anwendungsmöglichkeiten für Cloud-Computing im Handwerk könnten in verschiedensten Bereichen zum Einsatz kommen, zum Beispiel:

- Auftragserstellung/Auftragsverwaltung
- Mahn-/Rechnungswesen
- Dokumentverwaltung
- E-Mail-Dienste
- Lohnverwaltung
- Enterprise-Resource-Planning (ERP) (dt. Unternehmensressourcenplanung)
- Customer-Relationship-Management (CRM)
  (dt. Kundenbeziehungsmanagement)
- Lösungen für Steuerabrechnungen
- CAD-Anwendungen

Beispiele für Anwendungen in Handwerksbetrieben sind: Auftragserstellung, Mahn-/Rechnungswesen und Lohnverwaltung.

Anhand der folgenden Beispiele soll ein besseres Verständnis für die Identifizierung von positiven Merkmalen der Cloud-Service-Provider dargestellt werden.
Ein Hauptaugenmerk wird dabei auf die folgenden Punkte gelegt:

- Zertifizierungen
- Servicequalität
- Verschlüsselung
- Verfügbarkeit
- Nutzerverwaltung
- Monitoring
- Gerichtsstand

In den Beispielen wird exemplarisch ein Cloud-Service-Provider dargestellt, der eine Software auf Basis Software as a Service bereitstellt.

4.1.1 Software as a Service ï Handwerkslösungen: Positives Beispiel

Der Cloud-Service-Provider Good-Cloud bietet seinen Kunden ein zertifiziertes Rechenzentrum in Deutschland. Über eine freiwillige Zertifizierung auf Basis von ISO 27001 bestätigt dies auch eine dritte und unabhängige Instanz. Der weitere Bestand dieser Qualitätsauszeichnung wird alle drei Jahre auf ihre Gültigkeit hin überprüft, in dem das Rechenzentrum einen Rezertifizierungsprozess durchläuft.
Auf allen bereitgestellten Portalseiten des Cloud-Service-Providers wird eine https-verschlüsselte Verbindung im Browser des Nutzers vorausgesetzt. Durch eine hohe Übertragungsverschlüsslung wird das Entschlüsseln abgefangener Daten unmöglich.

Zertifizierte Cloud-Service-Provider haben hohe Standards in den Bereichen Verwaltung und IT-Sicherheit.

Mit einer Zwei-Faktor-Authentifizierung bietet der Cloud-Service-Provider einen zusätzlichen Schutz bei der Administration einer Cloud-Lösung. Dabei wird ein Zugriff auf ein System nur über die Nutzung von einem Passwort und zusätzlich über ein Hardware-Token in Form von einem USB-Dongle[16] ermöglicht.

Eine Verfügbarkeit von mindestens 99,9 % sollte durch einen Cloud-Service-Provider garantiert werden.

Weil die Firma Good-Cloud auch einen zusätzlichen Dienst zum Speichern von Daten in der Cloud bereitstellt, bietet sie ihren Kunden ein Programm zum Verschlüsseln hochgeladener Daten an. Der Kunde hat somit die Möglichkeit, Anhänge im Auftragssystem selbst zu verschlüsseln, bevor diese auf die Server des Cloud-Service-Providers gelangen. Alle weiteren Daten auf den Servern des Anbieters werden durch eine AES-Verschlüsselung gesichert.

In ihrem SLA positioniert sich die Firma Good-Cloud mit einer hohen Verfügbarkeit von 99,95 %. Dies bedeutet, dass im Durchschnitt eine maximale Ausfallzeit von 4,38 Stunden im Jahr nicht überschritten wird.

Verwenden Sie starke Passwörter.

Auf einem Internetportal des Cloud-Service-Providers kann ein Kunde komfortabel neue Nutzer erstellten und verwalten. Bei der Registrierung eines Accounts wird ein Einmalcode an die E-Mail-Adresse des neuen Nutzers versendet. Dieser kann nur zur einmaligen Registrierung verwendet werden und verfällt nach einer Stunde. Im Registrierungsprozess wird der Anwender auf die Relevanz von starken Passwörtern hingewiesen. Diese müssen den Mindeststandard von zehn Zeichen inklusive Sonderzeichen und Zahlen erfüllen.

Wählen Sie einen Cloud-Service-Provider aus, bei dem die Kosten transparent und übersichtlich zu jeder Zeit überprüft werden können.

Ebenso wird im Administrationsportal ein Bereich hervorgehoben, in dem der Kunde die aktuellen Kosten der genutzten Ressourcen und Lizenzkosten transparent einsehen kann und seine Gesamtkosten besser kalkulieren kann.

Wählen Sie Cloud-Service-Provider aus, die einen Gerichtsstand in Deutschland haben.

Der Hauptsitz der Firma ist in Deutschland, ebenso der Gerichtsstand. Die Firma wirbt bewusst mit den Vorteilen durch den hohen Datenschutz im Europäischen Wirtschaftsraum und besonders dem hohen Niveau in Deutschland.

In verschiedenen Bewertungsportalen im Internet hat die Firma Good-Cloud durchschnittlich sehr gute Bewertungen und wird von Kunden gelobt.

4.1.2 Software as a Service ï Handwerkslösungen: Negatives Beispiel

Cloud-Service-Provider Bad-Cloud hält sich auf seinem Internetauftritt sehr zurück, wenn es um Informationen über mögliche Sicherheitsstandards oder Zertifizierungen geht. Der Provider ist erst seit wenigen Monaten auf dem Markt.
Auf der Registrierungsseite kann ein Newsletter angefordert werden. In dem Formular wird zur Angabe persönlicher Informationen aufgefordert, die Daten werden jedoch unverschlüsselt an den Anbieter übertragen.

[16] USB-Dongle ï auch USB-Stick genannt, auf dem sich zusätzliche Authentisierungsmerkmale abgespeichert werden können

Der Anbieter stellt klar, dass es einen Kundendienst in Deutschland gibt. Dieser ist jedoch nur eingeschränkt verfügbar, weil sich das Unternehmen im deutschen Sprachraum noch in der Aufbauphase befindet. Eine Serviceverfügbarkeit wird daher nur auf Anfrage an den Kunden herausgegeben.

Vergleichen Sie Cloud-Services miteinander, um das sicherste und günstigste Angebot zu identifizieren.

Wie auch bei anderen Cloud-Diensten können in einem Administrationsportal Nutzer angelegt werden. Passwörter werden an neu angelegte Kunden per E-Mail versendet. Im Rahmen des Zertifizierungsprozesses muss das übermittelte Passwort nicht geändert werden.

Die Firma hat ihren Hauptsitz außerhalb des EWR, ebenso den Gerichtsstand.

In Bewertungsportalen sind hauptsächlich mittelmäßige Bewertungen zu erkennen, in denen sich Nutzer über die schlechte Erreichbarkeit des Kundendienstes beschweren.

4.1.3 Resümee der Beispiele

Im Folgenden werden die zuvor dargestellten Beispiele miteinander verglichen.

Zertifizierung

Cloud-Service-Provider Good-Cloud ist offenbar durch einen unabhängigen Dritten auf seine Standards im Bereich der IT-Sicherheit geprüft worden, ganz im Gegensatz zu Cloud-Service-Provider Bad-Cloud. Daraus lässt sich ableiten, dass bei dem positiven Beispiel Kapital für eine Verbesserung der IT-Sicherheit und die allgemeine Prozessstruktur investiert wurde. Es sollte zudem darauf geachtet werden, dass ein Unternehmen die Voraussetzungen für eine Rezertifizierung, die durchschnittlich alle zwei bis drei Jahre ansteht, erfüllt und durchläuft.

Eine gültige Zertifizierung bezeugt geprüfte Qualität durch einen Sachverständigen.

Übertragungsverschlüsselung

Rechtschreibfehler auf der Webseite des Anbieters können einen ersten Aufschluss über die Ernsthaftigkeit und Seriosität eines Cloud-Service-Providers vermitteln. Ein durchgängig, mittels https-geschützter Internetauftritt vermittelt ein Grundverständnis für mehr IT-Sicherheit in der Unternehmensstruktur, besonders wenn sensible Daten an den Cloud-Service-Provider übermittelt werden müssen. Falls im Registrierungsprozess auffällt, dass keine HTTPS-Übertragungsverschlüsselung aktiviert ist, sollte Vorsicht geboten sein.

SSL/TLS-Verschlüsselungen müssen vorhanden sein.

Kundenservice und Servicequalität

Achten Sie bei einer Cloud-Dienstleistung unbedingt auf eine im SLA geregelte Mindestverfügbarkeit bezüglich des Helpdesk-Services. Im Fall, dass es zu Problemen bei der Verfügbarkeit oder Fehlermeldungen bei einzelnen Diensten kommt, ist es wahrscheinlich, dass es zu hohen Wartezeiten kommt, wenn der Cloud-Service-Provider auf eine solche Situation nicht vorbereitet ist.

Kommt es zu Problemen bei der Nutzung eines Cloud-Services, ist die Erreichbarkeit des Kundendienstes wichtig.

Passwörter und Passwortqualität

Cloud-Service-Provider können mit einfachen Mechanismen Nutzer auf die Relevanz starker Passwörter hinweisen. Auch dies ist ein Indikator für ein erhöhtes IT-Sicherheitsbewusstsein. In dem negativen Beispiel muss ein Nutzer nach dem Erhalt einer Registrierungsnachricht kein neues Passwort vergeben. Dies kann dazu führen, dass unbekannte Dritte an das im Klartext übermittelte Kennwort gelangen. Mit einer zeitbeschränkten Änderung eines Kennwortes auf der Nutzerseite und den Hinweisen für starke Passwörter lassen sich diese Gefahren vermeiden.

Achten Sie bei der Auswahl eines Cloud-Anbieters insbesondere auf die im Folgenden dargestellten Kriterien.

- Verwendung der Technologien VPN und SSL/TLS für die Übertragungsverschlüsselung.
- Verschlüsselung der Daten bei einem Cloud-Service-Provider mittels AES.
- Die Möglichkeit einer Zwei-Faktor-Authentifizierung.
- Verfügbarkeit der Dienste und des Kundenservices.
- Hauptsitz in Deutschland oder dem Europäischen Wirtschaftsraum.
- Positive Kundenbewertungen.

4.1.4 Einzelne Dienstleistungen/Services aus der Cloud

Folgend werden weitere Dienstleistungen im Bereich von Cloud-Computing erläutert, die den Fokus auf IT-Sicherheit legen.

Web-Security aus der Cloud (SECaaS ï Security as a Service)

Bei einigen Cloud-Service-Providern können Sicherheitsfeatures hinzugebucht werden. Diese Dienste werden Security as a Service ge-nannt.

Security as a Service (SECaaS) oder auch Managed Security Services (MSS) genannt, beschreibt Dienste aus der Cloud, die die IT-Sicherheit der verwendeten Services verbessert.
Möglichkeiten sind hierbei das Nutzen von Antivirenpaketen, Spam-Erkennung oder Log-Monitoring. Diese Dienste können zu einem bestehenden Cloud-Dienst hinzugebucht werden, wenn es der Anbieter zur Verfügung stellt.

Empfehlungen

Kunden können sich über einzelne Angebote im Bereich von Security-Erweiterungen für spezifische Angebote direkt an den Cloud-Service-Provider wenden. Nicht jedes Cloud-Unternehmen bietet spezielle Sicherheitspakete und erweiterten Service an.

4.2 SaaS für Handwerksunternehmen

Im Folgenden werden beispielhaft Software as a Service Lösungen für das Handwerk dargestellt. Weitere sehr detaillierte Informationen können in der Studie des Fraunhofer Institut für Arbeitswirtschaft und Organisation entnommen werden.
http://wiki.iao.fraunhofer.de/images/studien/2012_cloudwerker_marktstudie.pdf

4.2.1 Weka Handwerksbüro

Das Weka Handwerksbüro (http://www.weka-bausoftware.de) ist eine kaufmännische Software speziell für das Bauhauptgewerbe, Ausbaugewerbe sowie das Handwerk für den gewerblichen Bedarf.
Die Cloud-Lösung von Weka bietet ein breites Sortiment an Funktionalitäten zum Beispiel in den Bereichen:

- Angebotserstellung,
- Auftragsverwaltung,
- Projektverwaltung,
- Rechnungsstellung,
- Zeiterfassung und
- Mahnwesen.

Mit einem Einrichtungsassistenten können erste Beispielprojekte erstellt werden. Zusätzlich gibt es eine ausführliche Hilfefunktion mit nützlichen Videos.

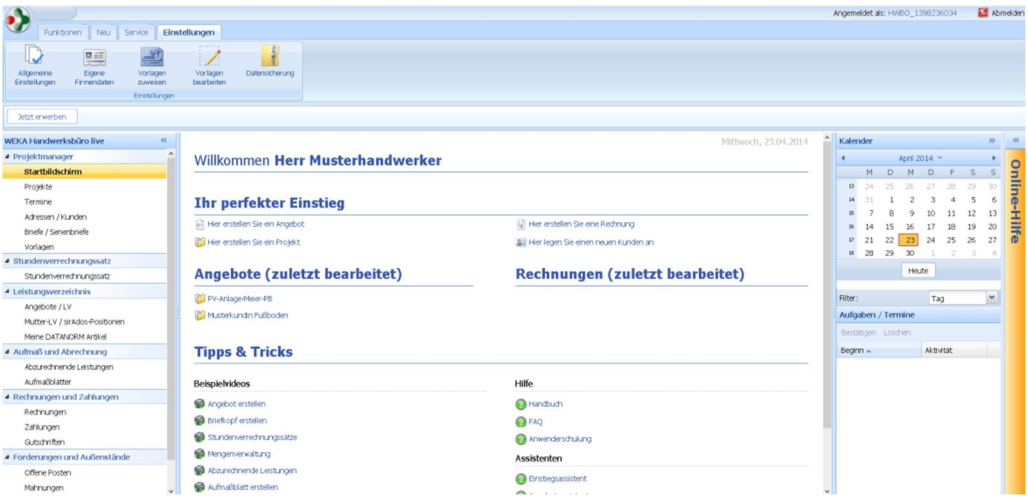


Abbildung 6: Weka Handwerksbüro

Kosten:

Die Kosten für die Software as a Service Version betragen monatlich ca. 50 ú pro Nutzer. Eine Einzelplatzlizenz ohne Cloudfunktionen ist für einmalig ca. 650 ú zu haben.

Datenstandort:

Weka nutzt ein Rechenzentrum in Deutschland mit dem Standort Kissing und unterliegt somit dem deutschen Datenschutzgesetz.

Systemvoraussetzungen:

Die Cloud-Variante von Weka benötigt lediglich einen aktuellen Browser, es wird speziell der Internet-Explorer oder Firefox empfohlen, um eine optimale Darstellung zu erreichen.

Empfohlene Bandbreite:

Es wird eine DSL-Anbindung empfohlen.

Testversion:

Es ist möglich einen kostenlosen Testzugang zu beantragen, dieser wird in weniger als einer Stunde bereitgestellt und kann sieben Tage lang ausgiebig getestet werden. http://www.handwerklive.de

4.2.2 Lexoffice

Lexoffice der Firma Haufe-Lexware GmbH & Co. KG (http://www.lexware.de) ist eine Software as a Service Lösung, mit der die Buchhaltung von Handwerksunternehmen überwacht werden kann.
Lexware bietet unter anderem folgenden Funktionsumfang:

- Angebotserstellung
- Auftragsverwaltung
- Rechnungsstellung
- Planung von Einnahmen und Ausgaben
- Einbindung von Online-Banking-Konten
- iPad App

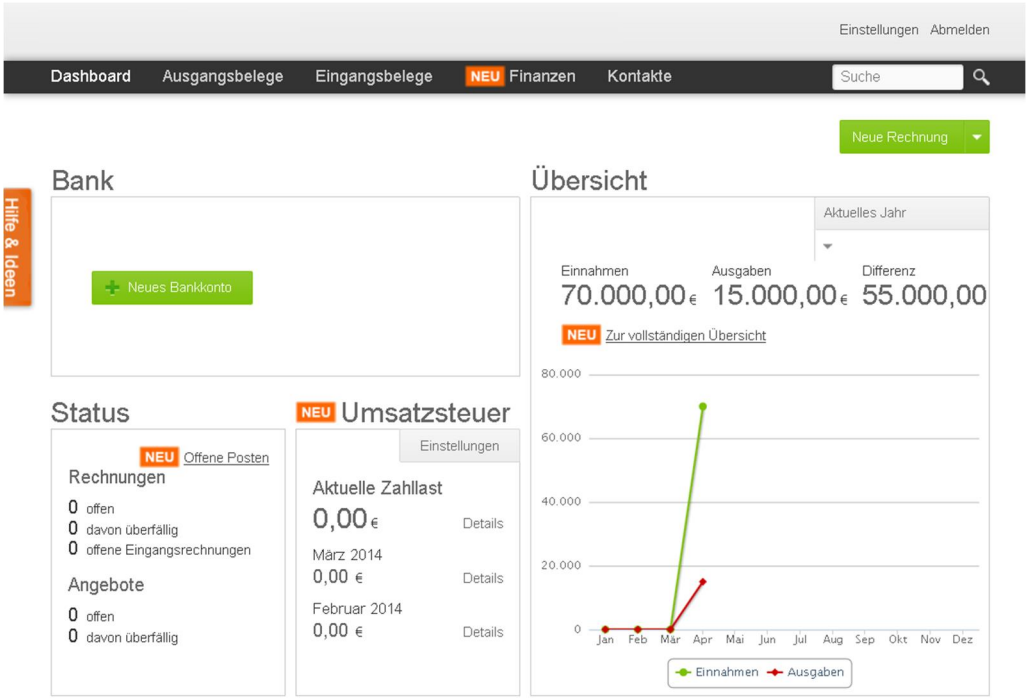


Abbildung 7: Lexoffice von Lexware

Kosten:

Es ergeben sich monatliche Kosten von 6 ú pro Nutzer im Basispaket Rechnung & Finanzen. Für 10 ú gibt auch das Basispakt und zusätzlich die Erweiterung für eine einfache Auftragsverwaltung. Die Mindestvertragslaufzeit beträgt einen Monat.

Datenstandort:

Der Speicherort der Daten befindet sich in einer nicht näher genannten Colocation in Deutschland und unterliegt den deutschen Datenschutzauflagen.

Systemvoraussetzungen:

Durch den Hersteller wird lediglich ein aktueller Browser verlangt, dies würde wie bei Weka beispielsweise einem aktuellen Firefox oder Internet-Explorer entsprechen.

Empfohlene Bandbreite:

Es wird eine DSL-Anbindung empfohlen.

Testversion:

Auch Lexoffice bietet eine kostenlose Testversion an, die sehr schnell bereitgestellt wird und über einen Zeitraum von 30 Tagen ausgiebig getestet werden kann.
http://www.lexoffice.de/registrierung

4.3 Leitfaden zur Entscheidungsfindung

In diesem Unterkapitel werden weitere wichtige Kriterien zur Entscheidungsfindung unter dem Gesichtspunkt der IT-Sicherheit dargestellt. Unter Einbezug der dargestellten Punkte soll dabei geholfen werden, Cloud-Service-Provider auszuwählen, die durch Zertifizierungen oder andere Merkmale eine ausgezeichnete Service-Qualität belegen können.

4.3.1 Auswahl Cloud-Anbieter

Nachdem bereits Beispiele für gute und schlechte Cloud-Dienstleister dargestellt wurden, werden nachfolgend Kriterien für eine Auswahl von Cloud-Service-Providern konkretisiert.

Zugangskriterien

Sichere Methoden für einen geschützten Zugriff sind das Bereitstellen von SSL-/TLS und VPN seitens des Anbieters.

Der Cloud-Service-Provider bietet einen Basisschutz für eine verschlüsselte Kommunikation zu den Cloud-Diensten. Diese bestehen zum Beispiel aus der Verwendung der HTTPS-Verschlüsselung und einem VPN-Zugang, mit dem die übertragenen Daten gegen Dritte abgesichert sind.
Bei der Einrichtung und der Registrierung der Nutzer wird auf die Verwendung von starken Passwörtern hingewiesen. Eine Eingabe von schwachen Passwörtern wird über eine Skala dargestellt.

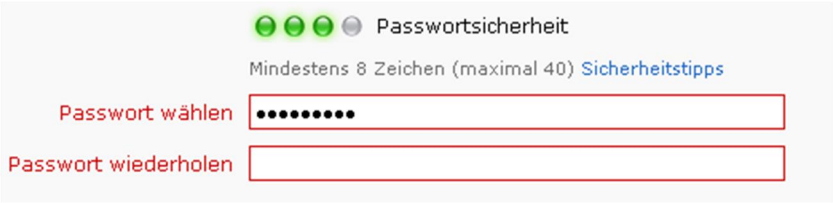


Abbildung 8: Erkennbare Passwortsicherheit

Bewertung eines Cloud-Anbieters recherchieren

Auf der Seite http://www.cloudsider.com können auch Bewertungs-Portale zu Rate gezogen werden. Hier sind verschiedene einschlägige Cloud-Dienste aufgelistet und bewertet. Leider finden sich zum aktuellen Stand dieses Handbuches noch keine Branchensoftwarelösungen aus dem Bereich Handwerk unter den bewerteten Cloud-Diensten. Für Branchensoftware kann der Ratgeber des Fraunhofer Instituts (s. Kapitel 4.2) zurate gezogen werden.

Kostenkalkulator

Der Cloud-Service-Provider sollte einen Kostenkalkulator zur Verfügung stellen, mit dessen Hilfe die aktuellen Kosten für Lizenzen, sowie Mehrkosten für Speicher oder Rechenkapazität transparent bestimmt werden können. Diese Rechnungshilfen finden Sie üblicherweise im Administrationsbereich oder auf Service-Portalen beim Anbieter.

Funktionsvergleich

Vergleichen Sie die Funktionen der Cloud-Anbieter miteinander, vergessen Sie dabei nicht wichtige Funktionen der IT-Sicherheit zu berücksichtigen, wie sie in Kapitel 4.1.3 dargestellt sind.
Hierfür können Sie wiederum die Webseite http://www.cloudsider.com benutzen.

Monitoring

Ein geeignetes Monitoring kann Ihnen eine treffende Aussage über Ihren aktuellen Datenverbrauch und Zugriffsstatistiken bereitstellen. Über das Monitoring ist es möglich zu erkennen, ob Ihre Ressourcen optimal genutzt werden.

Verschlüsselung

Ein gängiger Standard für Verschlüsselungen auf Festplatten ist der **A**dvanced **E**ncryption **S**tandard (**AES**), mit dem Daten vor unbekannten Dritten geschützt werden können.

Zugriffsarten (zum Beispiel WebDAV)

Web-based Distributed Authoring and Versioning (WebDAV) ist ein quelloffener Standard zum Bereitstellen von Dateien auf einem Server im Internet. Nutzer können mit Hilfe von WebDAV sehr einfach Ordner auf einem Internetserver ï wie einen Netzwerkordner ï anbinden. Dieser lässt sich über den Datei-Explorer ansteuern und öffnen.

Achten Sie bei der Nutzung von WebDAV unbedingt auf die Verwendung von Übertragungsverschlüsselung mittels HTTPS.

4.3.2 Zertifizierungen für Cloud-Dienste und ihre Bedeutung

Zertifizierungen unter dem Gesichtspunkt der IT-Sicherheit bestätigen ein grundlegendes und geprüftes Sicherheitsniveau durch unabhängige Dritte.
Bestimmte Zertifikate sind speziell für Cloud-Computing entwickelt worden. Wie sich diese Zertifikate in der Zukunft durchsetzen, bleibt abzuwarten. Dennoch ist eine Zertifizierung ein guter Indikator für einen hohen Stand der IT-Sicherheit oder ein geprüftes Informationssicherheits-Managementsystem.
In den folgenden Abschnitten werden einige grundlegende Zertifikate für die IT-Sicherheit bei Cloud-Computing und allgemeine Sicherheitsstandards dargestellt.
Zertifizierungen im Bereich Cloud-Computing bauen überwiegend auf lang etablierten Standards, wie beispielsweise ISO 27001, BSI-Grundschutz oder ITIL auf, siehe folgende Abschnitte.

ISO 27001

Bevor ein Cloud-Service-Provider eine Zertifizierung erhält, muss das Unternehmen die an die jeweilige Zertifizierung gestellten Kriterien erfüllen. ISO 27001 stellt normierte

ISO 27001 ist ein international anerkannter Standard für ein Informations-sicherheits-Management-system.

Anforderungen an ein Informationssicherheits-Managementsystem, dies betrifft insbesondere folgende Bereiche:

- Management von Sicherheitsvorfällen
- Sicherheit bei Personaleinsatz
- Management von Sicherheitslücken

Folgende Prozesse sind darüber hinaus in ISO 27001 definiert.

- Herstellung,
- Einführung,
- Betrieb,
- Überwachung,
- Wartung und
- Verbesserung

eines Informationssicherheits-Managementsystems (Terplan, 2011).

Diese Kriterien werden von einer vertrauenswürdigen Institution mit Hilfe eines Kriterienkatalogs überprüft und durch speziell ausgebildetes Fachpersonal in einem unabhängigen Audit zertifiziert.

BSI Grundschutz

Der BSI-Grundschutz ist in Kataloge unterteilt und deckt unteranderem die Bereiche Maßnahmen, Gefährdungen und Bausteine bei der Verwaltung und Administration von IT-Systemen ab.

Ein Grundstein für Maßnahmen im Bereich Vertraulichkeit und Verfügbarkeit kann mit einer Zertifizierung des Informationssicherheitsmanagements nach ISO 27001 auf der Basis des IT-Grundschutzes gelegt werden. Zu beachten ist, dass der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik[17] (BSI) bislang keine Cloud-Computing-spezifischen Kriterien enthält.
Im Juni 2013 kündigte das BSI an, bis Ende 2013 vier Bausteine speziell für Cloud-Computing zu erarbeiten (BSI, 2013).

IT Infrastructure Library ï ITIL

ITIL beinhaltet Best-Practice-Ansätze für die Konzipierung von IT-Infrastrukturen für Anbieter von IT-Systemen.

Die IT Infrastructure Library (ITIL) bietet so genannte Best-Practice-Ansätze für den Aufbau und Betrieb von IT-Infrastrukturen. ITIL gilt ähnlich ISO 27001 als international anerkannter Standard. Inhaltlich befasst sich ITIL mit folgenden Prozessen:

- Strategien zu Finanzen und Bedarfsabdeckung.
- Design von Verfügbarkeiten und Aufrechterhaltung des Betriebs.
- Best-Practices für die Veröffentlichung und Änderung von Prozessen.
- Operative Prozesse wie Vorfall- und Problem-Management.
- Service-Management und kontinuierliche Verbesserungsprozesse.

ITIL ist demnach ein Werkzeug für Anbieter von Cloud-Services.

[17] https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html

EuroCloud SaaS Star Audit[18]

Das EuroCloud SaaS Star Audit ist ein Gütesiegel speziell für Software as a Service-Anwendungen und wurde vom EuroCloud-Verband entwickelt.
Wird ein Cloud-Service-Provider mit einem SaaS Star Audit-Gütesiegel ausgezeichnet, wird dies transparent von einem bis fünf Sternen dargestellt. Ein Stern bietet eine Basisüberprüfung, fünf Sterne hingegen stellen eine sehr hohe Qualifizierung eines Cloud-Service-Providers dar.
Im Folgenden werden die verschiedenen Kategorien dargestellt, siehe (Thörner, 2011):

Anforderungen 1 Stern:

- Vertrag & Compliance[19]
  - Kündigungsregeln
  - Datenübergaberegelungen
  - Datenschutzanforderung
  - Datenlöschung bei Beendigung
- Betrieb Infrastruktur
  - Nachweis Minimalanforderungen Rechenzentrumbetrieb

Anforderungen 2 Sterne:

- Vertrag & Compliance
  - SLA Review
- Betrieb Infrastruktur
  - Nachweis Minimalanforderungen Rechenzentrum Betrieb Redundante Auslegung der Grundversorgung
- Anwendung
  - Schnittstellen, API, Exportformate

Anforderungen 3 Sterne:

- Vertrag & Compliance
  - Wahlmöglichkeit des Gerichtsstandes
- Implementierung
  - Implementierungskonzept
  - Bug Management
- OnSite Audit
  - Prüfung Service Level und Prozesse

Anforderungen 4 Sterne (gekürzte Darstellung):

- Vertrag & Compliance
  - Verfahrensdokumentation: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
- Sicherheit

---

[18] http://www.saas-audit.de/426/anforderungen
[19] *Compliance ist ein Themenfeld welches sich um die Einhaltung der geltenden Gesetze, Richtlinien und Vertragseinhaltungen befasst.*

    - Bereitstellung von VPN-Zugängen
    - Verschlüsselung der Nutzerdaten
    - Dateneinblick durch Administratoren ausgeschlossen?
    - Einbeziehen eines Kundensystems für Identitätsmanagement
    - Rechte- und Rollenvergabe durch den Kunden
- Betrieb Infrastruktur
    - Internet-Exchange Infrastruktur
    - Stromauslegung
    - Kühlung
- Betriebsprozesse
    - Störungsmanagement
    - Kapazitätsmanagement
    - Verfügbarkeitsmanagement
    - Service-Reporting

Anforderungen 5 Sterne (gekürzte Darstellung):

- Vertrag & Compliance
    - Prüfung des Preismodells
- Sicherheit
    - Durchführung von Penetrationstests
- Betrieb Infrastruktur
    - Notfallarbeitsplätze
    - Verteilte Rechenzentren (Geo-Redundanz)
- Betriebsprozesse
    - Notfallhandbuch
    - Notfallübungen

Weitere Zertifizierungen

TÜV Rheinland ï Certified Cloud Service[20]:
Der TÜV Rheinland bietet ein, auf der Basis von ISO 27001, ITIL und BSI-Grundschutz abgestimmtes, Zertifizierungskonzept speziell für Cloud-Services. Dabei werden unter anderem folgende Kriterien überprüft.

- Bewertung der Konzepte und Prozesse aus den Bereichen Hypervisor, Virtualisierung von Rechenzentren, Systeme, Zugriffskonzepte, Netzwerk, Systemschnittstellen, Administration, Service, Betrieb und Compliance
- In Interviews werden der Umsetzungsgrad, die Qualität und die Nachhaltigkeit der zuvor genannten Prozesse überprüft.
- Es werden SLAs hinsichtlich der Einhaltung des Leistungsversprechens untersucht.
- Mit Architekturanalysen wird die Belastbarkeit der Cloud-Service-Infrastruktur geprüft.
- In speziellen Penetrationstests werden die Anwendungen auf Sicherheitslücken überprüft.

[20] http://www.tuv.com/de/deutschland/gk/informationssicherheit_de/strategische_informationssicherheit/zertifizierungen_cloud_security/zertifizierungen_cloud_security.html

GERMAN CLOUD[21]

Ähnlich wie der TÜV Rheinland, konzentrieren sich die Prüfmethoden bei GERMAN CLOUD ebenso auf die etablierten Methoden rund um ISO 27001, ITIL und BSI-Grundschutz. GERMAN CLOUD ist ein Zusammenschluss von öffentlichen Datenschützern, dem Berufsverband der Datenschützer sowie der Universität Koblenz.
Unter anderem wird auf folgende Kriterien geprüft:

- Verbindlichkeit der Geschäftsleitung
- Verantwortliche für Datenschutz gem. BDSG
- Organisatorische Schutzregeln
- Technische Bedingungen
- Qualitätskontrollen, Zugang, Zutritt
- SLA und Leistungsversprechen

4.3.3 Mitarbeiter-Sensibilisierung

Warum ist eine Mitarbeiter-Sensibilisierung in puncto Cloud-Computing wichtig?
Die Problematik ergibt sich aus einem Wildwuchs im Unternehmen, der durch die Nutzung von verschiedenen Cloud-Diensten entstehen kann.
Speicherlösungen, die es einem Nutzer ermöglichen, seine Daten kostenlos zu speichern, werden von verschiedensten Anbietern beworben. Dies sollte kritisch hinterfragt werden, da sich die Frage ergibt, wo die Daten gespeichert werden. Zusätzlich muss bedacht werden, welchen Datenschutzgesetzen diese kostenfreien Dienste unterliegen.
Nutzt ein Mitarbeiter eine ausländischen Storage as a Service-Lösung für private Zwecke außerhalb des Unternehmens, ist es die Aufgabe des jeweiligen Mitarbeiters, sich über die Datenschutzbedingungen zu informieren.
Anders sieht es aus, wenn ein Mitarbeiter Unternehmensdaten auf einem Cloud-basierten Speichersystem ablegt. Hier können im schlechtesten Fall personenbezogene Kundendaten, die dem deutschen Datenschutz unterliegen, in ein anderes Land abfließen. Der Datenschutz dieser Informationen kann somit nicht mehr gewährleistet werden.

Klären Sie Mitarbeiter über potenzielle Risiken bezüglich des Datenschutzes, sowie der Benutzung von privaten Cloud-Diensten auf.
Es sollten ausschließlich unternehmensintern abgestimmte Cloud-Services verwendet werden, die durch die Geschäftsführung zugelassen sind.

[21] http://www.saas-audit.de/426/anforderungen

4.4 Zusammenfassung

In diesem Kapitel wurden beispielhaft die Unterschiede zwischen einem positiven und einem negativen Angebot dargestellt. Dabei wurde insbesondere auf die wichtigen Bereiche der Übertragungsverschlüsselung, Zertifizierung, Verfügbarkeit und Passwortqualität bei Cloud-Dienstleistungen eingegangen. Darüber hinaus wurden in einem Leitfaden zur Entscheidungsfindung Merkmale für die Auswahl von sicheren Cloud-Service-Providern zusammengefasst.
Im Abschnitt Zertifizierungen wurden allgemeine Zertifizierungen und ein speziell auf Software as a Service zugeschnittenes Gütesiegel dargestellt. Das Thema Mitarbeiter-Sensibilisierung beschrieb die Problematik, die durch privat genutzte Cloud-Dienste im Unternehmen entstehen kann.

5. Compliance & Recht

In den folgenden Kapiteln erhalten Sie einen Einblick in die Bereiche Compliance und Recht. Sie werden unter dem Gesichtspunkt des Deutschen und Europäischen Datenschutzes betrachtet.

5.1 Vertragsrechtliche Bestimmungen

Zu jedem Cloud-Service gehört ein entsprechender rechtsgültiger Vertrag zwischen Cloud-Service-Provider und Nutzer. In diesem werden alle Rechte und Pflichten der einzelnen Parteien festgehalten.

5.1.1 Allgemeine Geschäftsbedingungen (Leistungsschuld)

Die Leistungsschuld beim Cloud-Computing trägt der Cloud-Service-Provider. Er ist dazu verpflichtet, die Dienste für einen Nutzer erreichbar zu halten. Mögliche Dienste sind Datenbanken, Selbstservice-/Administrationsportale, Anwendungen und Datenspeicher.

Der Cloud-Service-Provider trägt eine Leistungsschuld und muss die Verfügbarkeit von Cloud-Services gewährleisten.

Die Grundlage für diese Leistungsschuld begründet sich aus einem Urteil des Bundesgerichtshofes, bei dem ein Application Service Provider (ASP) bzw. Cloud-Service-Provider eine Leistungsschuld an den Nutzer der Dienste trägt.

Demnach heißt es in dem Urteil (Smith, 2007):

ĂDer zwischen den Parteien abgeschlossene ASP-Vertrag sei ein Vertrag eigener Art, auf den im Wesentlichen Mietvertragsrecht anzuwenden sei. Bei ASP-Verträgen sei die Software auf dem Server des Anbieters gespeichert, sodass sie als Sache im Sinne von § 90 BGB anzusehen sei. Die Software werde vom Anbieter dem Kunden auch im Sinne von § 535 Abs. 1 Satz 2 BGB[22] überlassen, indem er sie ihm über das Internet zur Nutzung zur Verfügung stelle.ñ

5.1.2 Lizenzierung von Software in der Cloud

Bei Software as a Service werden andere Verteilungswege eingeschlagen als bei klassischen Softwareprodukten, dennoch gelten auch für Softwareprodukte aus der Cloud die gleichen Gesetzmäßigkeiten, die im deutschen Urheberrechtsgesetz (UrhG) niedergeschrieben sind.

Besonders hervorzuheben sind § 69a Abs. 1 und Abs. 2 UrhG:
ĂComputerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.ñ

[22] *§ 535 Inhalt und Hauptpflichten des Mietvertrags Abs. 1 Satz 2 BGB:*
Ă(2) Der Mieter ist verpflichtet, dem Vermieter die vereinbarte Miete zu entrichten.ñ

ĂComputerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, daß sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.ñ

Der Cloud-Service-Provider kann demnach einem Kunden ein Nutzungsrecht über eine gewisse zeitliche Periode einräumen.
In einem Vertrag zwischen Cloud-Service-Provider und Kunden werden zumeist folgende Nutzungsrechte festgelegt.

Die Lizenzierung bei Software as a Service unterliegt dem Urhebergesetz, Art der Nutzung, Nutzungszeitraum und geografisch eingeschränkte Nutzungsrechte werden durch einen Anbieter bestimmt.

- Nutzungsgegenstand und Art der Nutzung:
  Der Nutzungsgegenstand ist die Software und alle dazu gehörenden Merkmale. Dabei wird auch festgelegt, durch wen die Software verwendet werden darf.

- Nutzungszeitraum:
  Es wird eine Periode festgelegt, in der ein Kunde eine Applikation über Software as a Service beziehen und nutzen darf.

- Begrenzung der Rechte durch eine geografische Beschränkung:
  Einige Applikationen können auf bestimmte Rechtsräume, wie beispielsweise Deutschland oder den Europäischen Wirtschaftsraum, beschränkt werden.

Nutzungsmodelle

Nutzungsmodelle können unter anderem Volumenlizenzen oder Einzellizenzen sein. Dabei wird häufig eine Vergünstigung für die Abnahme von Volumenlizenzen angeboten. Dies bietet Einsparpotenzial für Unternehmen, die ein größeres Kontingent an Applikationen nutzen.

5.2 Service Level Agreement

Bei einem Service Level Agreement (SLA) wird die Qualität der Dienste zwischen dem Cloud-Service-Provider und einem Kunden definiert. Dabei stellt der Kunde eine Anforderung an die Qualität, zum Beispiel die Verfügbarkeit, die zusätzlich zu einem Rahmenvertrag verfasst wird. Der Cloud-Service-Provider gewährleistet diese mit einer konkreten Aussage: Zum Beispiel der Angabe, wie hoch die Ausfallsicherung seiner Services im Durchschnitt auf 365 Tage im Jahr ist. Andere wichtige Services sind die Erreichbarkeit von Servicemitarbeitern im Kundensupport, diese können ebenfalls in einem SLA festgelegt werden.

In einem SLA wird einem Mindestmaß an Servicequalität vertraglich geregelt. Bei Nichteinhaltung vertraglicher Kriterien besteht das Recht auf Schadensersatz.

Wenn die im SLA geforderten Mindestanforderungen vom Cloud-Service-Provider nicht erfüllt werden, hat der Dienstnutzer einen Anspruch auf Schadensersatz.

Eine spezielle Form ist das Security Service Level Agreement (SSLA), in dieser Vereinbarung wird die Servicequalität für die IT-Sicherheit festgeschrieben.

5.2.1 Was ist bei Service Level Agreements zu beachten?

Bei der Nutzung von SLAs ist zu beachten, dass bei der Verwendung von Public-Cloud-Diensten zumeist standardisierte Fassungen angeboten werden, die kleinere Kunden nicht anpassen können (s. Kapitel 5.2.2). Gerade deswegen ist es obligatorisch abzuwägen, ob Mindestanforderungen durch die allgemeinen SLA abgedeckt werden.
Folgende Punkte sind bei jedem SLA zu beachten:

In einem SLA werden Key Performance Indicators (KPI) dargestellt, diese bestehen aus:

- Verfügbarkeit der Dienste in einem zeitlich eindeutigen Messraum
- Reaktionszeit auf Störungen seitens des Supports
- Zeitraum für die Beseitigung von Fehlern

Weitere allgemeine Angaben sind (Terplan, 2011):

- Ort und Datum
- Ziel des SLA
- Laufzeit des SLA
- Prioritäten im SLA
- Standorte
- Organisationseinheiten
- Anwendungen
- Dienstzeiten zur Erbringung der Dienstleistungen (7 x 24 x 365)

Es gibt auch Zustände, die eine Erfüllung des SLA beeinträchtigen können, diese könnten unter anderem durch Katastrophen, Sabotage oder Maßnahmen für eine Instandhaltung verwandter Hardwarekomponenten veranschlagt werden.

Vereinbaren Sie ein klar definiertes Service Level Agreement mit einem Cloud-Service-Provider.

5.2.2 Klassifizierung SLA

SLA können in zwei Kategorien unterteilt werden: Individuelle SLA und standardisierte SLA, wie im Folgenden dargestellt wird.

Individuelle SLA

Die Erarbeitung von auf Kunden zugeschnittene SLA, bedeutet einen hohen Verwaltungsaufwand bei dem Cloud-Service-Provider.
Wenn große Unternehmen Cloud-Dienstleistungen in Anspruch nehmen, ist es für diese möglich, den Aufwand zu stemmen und maßgeblich an der Individualisierung der SLA mitzuwirken. Bei Handwerksunternehmen fehlen häufig Ressourcen hierfür.

Es gibt individuelle und standardisierte Service Level Agreements, individuelle SLA können angepasst werden, standardisierte SLA hingegen nicht.

Aus diesem Grund ist es für Handwerksunternehmen überwiegend nicht möglich, ein individuelles SLA zu verlangen. Dies kann jedoch individuell unterschiedlich sein und sollte während der Verhandlung über ein Angebot mit einem Cloud-Service-Provider einbezogen werden.

Standardisierte SLA

Handwerksunternehmen müssen zumeist auf standardisierte Exemplare der SLA zurückgreifen, dabei gilt es die in Kapitel 5.2.1 aufgeführten wichtigsten Kriterien zu beachten, damit ein Mindestniveau für ein SLA mit einem Cloud-Service-Provider erfüllt wird.

Bei der Einschätzung von Standardisierten Service Level Agreements können auch Gütesiegel, wie das EuroCloud Star Audit, bei einer Einschätzung unterstützen, wenn ein solches Gütesiegel ausgestellt wurde.

5.3 Was ist beim Anbieterwechsel zu beachten?

Der wohl wichtigste Punkt bei einem Anbieterwechsel ist, einen Wechsel schon vor dem Vertragsabschluss bzw. vor der Nutzung eines Cloud-Dienstes bedacht zu haben. Dabei geht es um Vertragsdetails, die in jedem Service-Vertrag erarbeitet werden sollten, unter anderem:

- Rückführbarkeit und Rückgabeformat
- Sicheres Löschen der Daten

5.3.1 Rückgabeformat der Daten bei Vertragsbeendigung

Zu Beginn einer Vertragsbindung sollten Konzepte erarbeitet werden, um eine geregelte Vertragsbeendigung (engl. Exit-Management) zu ermöglichen. Dieses Konzept verhindert, dass ein Cloud-Nutzer bei einem Anbieter eingeschlossen wird (engl. Vendor lock-in). Im Exit-Management müssen Strategien und Maßnahmen erarbeitet werden, um eine Vertragsbeendigung schnell und sicher abwickeln zu können (Janser, 2012).
Ein Beispiel für so einen Fall ist die Nutzung von ĂSoftware as a Serviceñund der damit einhergehenden Speicherung von Daten im Rechenzentrum des Anbieters. Dabei ist ein kompatibles Rückgabeformat der Daten ein essenzieller Bestandteil. Hiermit wird die Voraussetzung geschaffen, einen Wechsel zu einem anderen Cloud-Service-Provider oder in eine Private-Cloud zu ermöglichen.
In der Vertragsbeendigung sollte auch festgelegt sein, dass der Cloud-Service-Provider alle erhobenen Daten sicher aus allen Systemen löschen muss.

Achten Sie vor einem Vertragsabschluss auf ein standardisiertes Rückgabeformat.

5.3.2 Daten komplett aus der Cloud löschen

Um Daten sicher aus der Cloud löschen zu können, muss vertraglich festgelegt werden, wie ein solcher Vorgang durchzuführen ist. Ein Cloud-Service-Provider kann zum Beispiel anbieten, die Daten und alle gespeicherten Backups durch Mehrfachüberschreibungen der Daten so zu überschreiben, dass kein Wiederherstellen möglich ist.

5.4 Einheitliche Standards für Cloud-Computing

Cloud-Computing setzt sich bereits seit mehreren Jahren auf dem internationalen und nationalen Markt durch. Durch die hohe Menge an Anbietern ist es jedoch zu einer breiten Fächerung an Eigenentwicklungen durch die Cloud-Service-Provider gekommen. Führend dabei sind US-Unternehmen, die durch ihre hohe Marktverbreitung und Macht versuchen, ihre eigenen Standards durchzusetzen.
Dies geht aus einer Studie des Bundesministeriums für Wirtschaft und Technologie (BMWi) hervor (Dr. Rainer Bernnat et al., 2012). In dieser Studie wurden 19 der wichtigsten Normierungs- und Standardisierungsorganisationen erfasst und betrachtet. In Deutschland tragen folgende Organisationen einen Beitrag:

- Deutsches Institut für Normung ï DIN
- SaaS-EcoSystem
- Euro-Cloud Deutschland

International wird laut Studie das National Institute of Standards and Technology ï NIST gesehen.

5.5 Datenschutzrechtliche Anforderungen

In Anbetracht der umfassenden Abhörskandale, die im Jahr 2013 aufgedeckt wurden, sind Cloud-Computing-Dienste, die ihren Gerichtsstand oder Hauptsitz außerhalb der EU bzw. des Europäischen Wirtschaftsraumes haben, ausdrücklich nicht zu empfehlen. Grund ist, dass außerhalb der EU nicht das Europäische Datenschutzgesetz durchgesetzt werden kann. Auch eine Vereinbarung wie Safe Harbor, die zwischen den USA und dem Europäischen Wirtschaftsraum geschlossen wurde, wird weitestgehend durch europäische und deutsche Datenschützer kritisch beäugt (Die Landesbeauftragte für Datenschutz, 2013). Dies hat ausdrücklich zur Folge, dass alle Dienste außerhalb des EWR nicht ausreichend geschützt werden können.

5.5.1 Datenschutz in Deutschland und Europa

Die Europäische Datenschutzrichtlinie 95/46/EG (EU-DSRL) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde 1995 von der EU erlassen. Diese Richtlinie garantiert einen EU-weiten rechtlichen Rahmen für den Schutz und Bedingungen für die Übermittlung von personenbezogenen Daten.

Daten innerhalb Europas unterliegen der Europäischen Datenschutz-verordnung.

Richtlinien dieser Art sind von den Mitgliedsstaaten innerhalb von festgesetzten Fristen zu erfüllen. Werden diese Fristen nicht eingehalten, müssen betroffene Staaten mit einem so genannten Vertragsverletzungsverfahren rechnen. Hierbei ist das Verfahren beispielsweise gegen Deutschland im Jahr 2010 zu erwähnen.

Durch diese Mindestanforderungen an den Datenschutz sind hohe Standards bei der Verarbeitung von Daten und besonders bei der Verarbeitung von personenbezogenen Daten festgeschrieben.

5.5.2 Datenschutz außerhalb Europas

Da die Cloud-Computing Industrie maßgeblich von US-Amerikanischen Unternehmen geprägt wird, wird in den folgenden Unterkapiteln speziell auf die Problematik bei dem Datenschutz zwischen den USA und Europa eingegangen.

Safe Harbor

Das Safe Harbor-Abkommen wird im Zuge des NSA-Skandals in Frage gestellt.

Safe Harbor ist die Datenschutzvereinbarung zwischen dem EWR und den USA. Sie wurde erarbeitet, da die USA bis zum Jahr 2000 kein adäquates Datenschutzniveau für den Austausch und die Verarbeitung von personenbezogenen Daten besaß, so wie es in Art.25 Abs. 1 EU-DSRL gefordert wird. Dementsprechend einigten sich die EU und die USA, in Verhandlungen nach Art. 25 Abs. 5 EU-DSRL, auf eine Festlegung von Richtlinien, die in Safe Harbor festgelegt wurden.
Das Recht für diese Maßnahme leitet sich aus Art. 25 Abs. 6 EU-DSRL ab, in dem ein Drittland das Recht auf eine Neubewertung durch die in Artikel 25 Abs. 2 EU-DSRL festgelegten Kriterien hat.

Die Konformität zu Safe Harbor wird bei US-Unternehmen durch eine Selbstzertifizierung vorgenommen, bei der sie sieben Prinzipien und die so genannten 15 Frequently Asked Questions wahrheitsgemäß zu beantworten haben (Der Bundesbeauftragte für den Datenschutz, 2013).
Bezüglich Cloud-Computing sind hier keine expliziten Aussagen zu finden, dennoch sind die im Folgenden aufgezählten Kriterien wichtige Punkte für den Datenschutz und die Datensicherheit bei der Nutzung von US-Cloud-Anbietern.
Kritikpunkte an Safe Harbor und der Selbstzertifizierung werden im Abschnitt Patriot Act erbracht.
Die sieben Prinzipien zur Selbstzertifizierung besagen folgendes:

Informationspflicht
Personen, über die Daten erhoben wurden, haben das Recht auf Auskunft darüber, zu welchem Zweck Daten erhoben und ob sie an Dritte weiter geleitet werden sollen. Es muss das Recht auf Untersagung bestehen, bevor Daten zu einem anderen Zweck weitergegeben werden. Stellen für Beschwerden oder Nachfragen diesbezüglich müssen öffentlich für die Besitzer der Daten annonciert werden.

Wahlmöglichkeit
Nutzer müssen die Möglichkeit haben, eine Weitergabe von Daten an Dritte zu untersagen. Dies gilt besonders bei sensiblen Datenangaben über Ă[...] den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben [...]ñ

Weitergabe
Daten dürfen nur unter Berücksichtigung der Informationspflicht weiter gegeben werden. Wurde die Informationspflicht erteilt, muss das Unternehmen, an welches die Daten weiter gegeben werden entweder selbst Safe Harbor zertifiziert sein oder es muss eine Feststellung bezüglich des angemessenen Schutzniveaus erfasst werden. Das Schutzniveau muss wiederum Safe Harbor konform sein.

Sicherheit
Das Unternehmen verpflichtet sich, Daten vor Verlust, Missbrauch und unbefugtem Zugriff, sowie Weitergabe, Änderung und Zerstörung zu schützen.

Datenintegrität
Daten müssen zuverlässig, genau, vollständig und aktuell sein, dieses muss ein Unternehmen mit geeigneten Maßnahmen garantieren.

Auskunftsrecht
Es muss der Zugang für Privatpersonen realisiert sein, damit diese Daten korrigieren, ändern oder löschen können, wenn sie falsch sind. Es sei denn, die Kosten für die Einrichtung eines Zugangs würde sich nicht mit den Nachteilen für den Besitzer der Daten decken.

Durchsetzung
Unternehmen verpflichten sich dazu, Personen die Möglichkeit zu bieten, ihr Recht auf Privatsphäre prüfen zu können. Dieses beinhaltet die Anwendung von Rechtsmaßnahmen und im Falle der Nichteinhaltung der Safe Harbor Bestimmungen, das Recht auf Schadensersatz.

Patriot Act

Im Jahr 2001 wurde nach den Terroranschlägen am 11. September in New York der PATRIOT ACT von der US-Regierung unter der Führung des damaligen US-Präsidenten George W. Bush entworfen. Dieser sollte die Bürgerrechte beschneiden und die Rechte der Ermittlungsbehörden, wie beispielsweise FBI und CIA ausbauen, um den Staat, seine Einrichtungen und die Bürger effektiver vor Terror schützen zu können.

Der nach den Terroranschlägen vom 11. September 2001 verabschiedete Patriot Act hebt die in Safe Harbor vereinbarten Datenschutzbestimmungen auf.

Dabei wurde das Ermittlungsrecht soweit ausgebaut, dass US-Unternehmen mit Datencentern in der EU auf Anfrage der US-Regierung oder US-Ermittlungsbehörden, jegliche personenbezogene Daten über eventuelle Verdächtige herausgeben müssen.
Dies geht soweit, dass es bei einem verordneten Redeverbot (gag order) sogar unter Androhung von Strafe verboten ist, Details über solche Herausgaben zu veröffentlichen (Beverley Becker et al., 2010, S. 365 ff.).
Diese Fakten verstoßen demnach gegen die Informationspflicht, wie sie in der Safe Harbor Richtlinie gefordert ist.
Fälle in denen es zu Herausgaben dieser Daten und der Erteilung von Redeverboten gekommen ist, wurden durch große Amerikanische Cloud-Service-Provider bestätigt.

PRISM/Tempora/Xkeyscore

Durch den im Jahr 2013 aufgedeckten Spionageskandal mit den verschiedenen Werkzeugen, zum Beispiel PRISM (USA), Tempora (Großbritannien) und XKeyscore wurde das Vertrauen in ausländische Cloud-Anbieter gravierend verletzt.

Daten auf Servern der beteiligten Nationen sind demnach unter ständiger Überwachung der verschiedenen Geheimdienste.

5.6 Zusammenfassung

Amerikanische und britische Abhörmaßnahmen haben das Vertrauen in Cloud-Computing stark geschwächt. Die Verwendung von Cloud-Diensten aus diesen Ländern sollte daher ausgeschlossen werden.
Bei der Verwendung von inländischen Cloud-Services ist vor einem Vertragsabschluss der geltende Datenschutz zu beachten.
Nutzer von Cloud-Diensten tragen die Verantwortung zur Prüfung, ob ein Mindeststandard an Datenschutz durch einen Cloud-Service-Provider gewährleistet wird.

6. Checkliste ĂCloud-Computingñ

IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

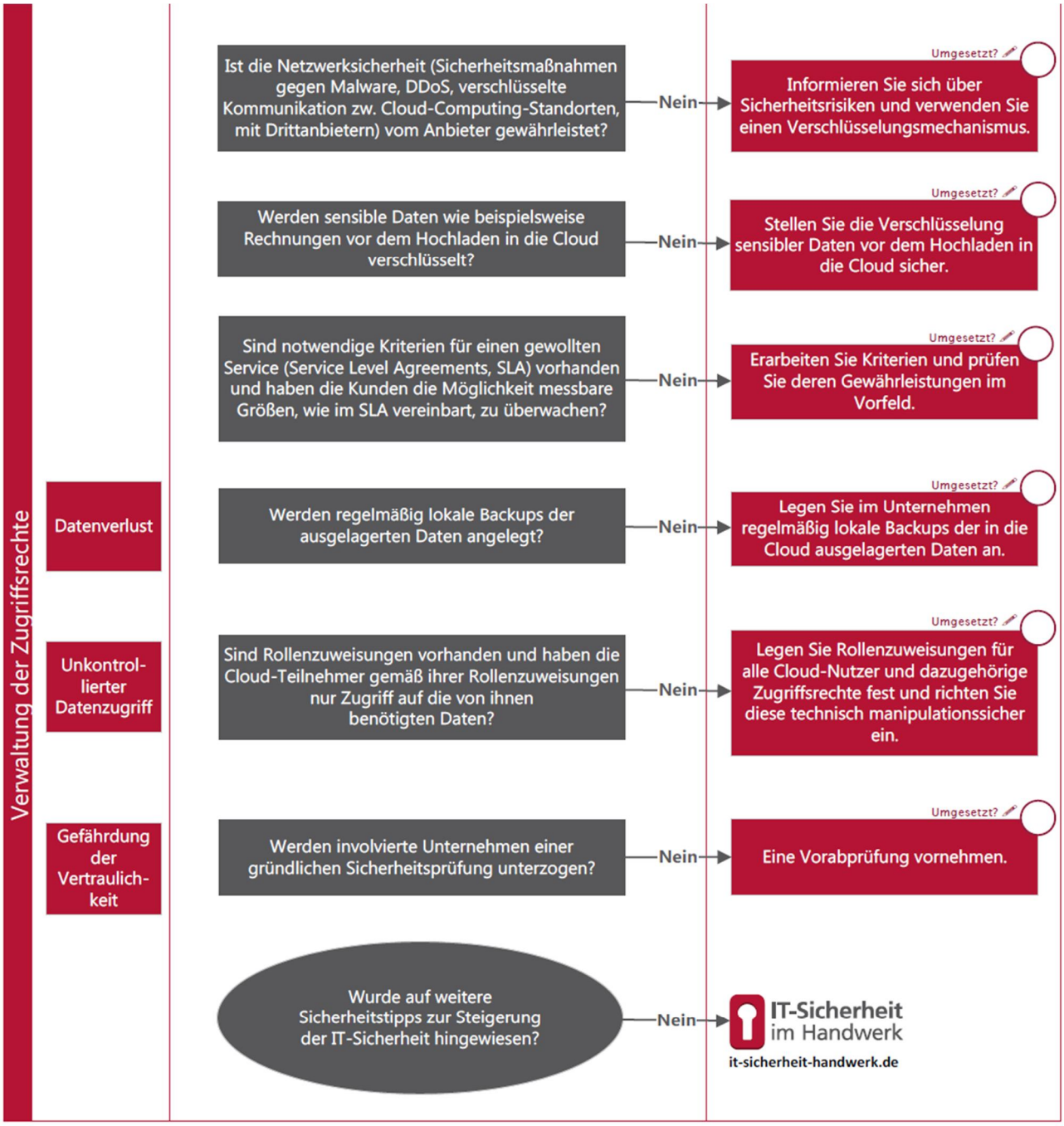
Bundesministerium für Wirtschaft und Energie

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

aufgrund eines Beschlusses des Deutschen Bundestages

Sichere Ablage in der Cloud

	Gefahr/ Risiko	Erhebung des Ist-Zustands		Maßnahme
Klassifizierung vertraulicher Informationen	Angriffe durch Schad-programme	Verfügen die für den Datenaustausch mit der Cloud vorgesehenen Geräte (PC, Smartphone, Tablet) über einen ausreichenden Basisschutz, inklusive Viren-Schutz, Personal Firewall und weiterer Sicherheitsanwendungen wie beispielsweise die „securityNews"-App?	Nein →	Umgesetzt? Mit Hilfe der Checkliste „Basisschutz" überprüfen.
	Verlust der Datenhoheit	Gibt es im Unternehmen Richtlinien zur Klassifizierung vertraulicher Daten?	Nein →	Umgesetzt? Entwickeln Sie Richtlinien zur Klassifizierung vertraulicher Daten, definieren Sie Vertraulichkeitsstufen und sichern Sie die durchgängige Anwendung dieser.
	Verlust vertraulicher Daten	Wurden mit der Klassifizierung vertraulicher Daten Speicherorte für diese Daten festgelegt?	Nein →	Umgesetzt? Fordern Sie die Mitarbeiter auf, hochsensible Daten wie Strategien oder Konstruktionspläne niemals mit der Möglichkeit durch Zugriff Dritter zu speichern; Speicherorte sollten anhand der Vertraulichkeitsstufen festgelegt werden.
Datenschutz	Verlust der Datenhoheit	Werden die Serverstandorte des Cloud-Service Anbieters (Land, Region), an denen die Daten gespeichert und verarbeitet werden, offengelegt? Handelt es sich um einen Anbieter mit Unternehmenssitz und Serverstandort in Deutschland?	Nein →	Umgesetzt? Bei Cloud-Anbietern mit Unternehmenssitz/ Serverstandort außerhalb Deutschlands bestehen Sicherheitsrisiken. Sie sollten daher von diesen Anbietern absehen.
Sicherheitsbedingung des Anbieters	Gefährdung der Verfügbarkeit	Handelt es sich um einen kostenpflichtigen Service?	Nein →	Umgesetzt? Hinterfragen Sie kostenlose Angebote kritisch und wechseln Sie ggf. zu einem anderen (kostenpflichten) Anbieter.
		Fallen unabhängige Test- und Presseberichte für diesen Anbieter positiv aus?	Nein →	Umgesetzt? Prüfen Sie die Möglichkeiten eines Wechsels zu einem besser bewertetem Anbieter.
	Gefährdung der Vertraulich-keit	Sprechen die AGB des Anbieters und das Thema 'Datenschutz' für den Anbieter? Besteht ein Kontrollrecht/-Weisungsrecht oder das Testat eines unabhängigen Sachverständigen?	Nein →	Umgesetzt? Ziehen Sie einen Wechsel zu einem anderen Anbieter in Betracht, der diese Bedingungen erfüllt.



TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Task Force „IT-Sicherheit in der Wirtschaft“
Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de

itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is) - Institut für Internet-Sicherheit der Westfälischen Hochschule

7. Weblinks

- http://www.it-sicherheit-handwerk.de
- https://www.internet-sicherheit.de
- http://www.heise.de
- https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html
- http://keepass.info
- http://www.truecrypt.org
- https://owncloud.org
- http://www.cloudsider.com
- http://wiki.iao.fraunhofer.de/index.php/Marktstudie:_Cloud-Lösungen_für_das_Handwerk
- http://www.cloudwerker.de

8. Literaturverzeichnis

Stand der IT-Sicherheit im Handwerk (2013).

Andreas Wilkens (2009): Sidekick-Datenverlust wirft Schatten auf die "Cloud". Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/newsticker/meldung/Sidekick-Datenverlust-wirft-Schatten-auf-die-Cloud-821328.html, zuletzt geprüft am 07.11.2013.

BITKOM (2009): Cloud Computing - Evolution in der Technik, Revolution im Business. Online verfügbar unter http://www.bitkom.org/files/documents/bitkom-leitfaden-cloudcomputing_web.pdf, zuletzt geprüft am 22.08.2013.

Björn Greif (2013): Dropbox-Nutzer von Spamwelle betroffen. Hg. v. zdnet.de. Online verfügbar unter http://www.zdnet.de/88145766/dropbox-nutzer-von-spamwelle-betroffen/, zuletzt geprüft am 12.11.2013.

BSI (2013): Sichere Cloud-Lösungen bringen mehr Wettbewerbsfähigkeit. BSI kündigt IT-Grundschutz-Bausteine für Cloud Computing an. Bundesamt für Sicherheit in der Informationstechnik (BSI). Online verfügbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/IT-Grundschutz-Bausteine_Cloud_Computing_25062013.html.

Der Bundesbeauftragte für den Datenschutz (2013): Safe Harbor. Online verfügbar unter http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html?nn=409532, zuletzt geprüft am 26.08.2013.

Die Landesbeauftragte für Datenschutz (2013): Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten. Der Bundesbeauftragte für den Datenschutz. Online verfügbar unter http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html?nn=408908, zuletzt geprüft am 26.08.2013.

Dr. Rainer Bernnat; Dr. Wolfgang Zink; Dr. Nicolai Bieber; Joachim Strach (2012): Das Normungs- und Standardisierungsumfeld von Cloud Computing. Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms ĂTrusted Cloudñ, zuletzt geprüft am 14.11.2013.

Fraunhofer IESE (2011): Cloud Computing 2011. Ziele, Bedenken und Fragestellungen hinsichtlich Softwareentwicklung. Institut für Experimentelles Software Engineering IESE, zuletzt geprüft am 22.08.2013.

Janser, Hinzpeter (2012): So gelingen Outsourcing-Verträge. Exit-Management. Hg. v. computerwoche.de.

Matt Hickey, Stefan Beiersmann (2009): Serverfehler führt zu Datenverlust bei Sidekick-Nutzern. Hg. v. zdnet.de. Online verfügbar unter http://www.zdnet.de/41515639/serverfehler-fuehrt-zu-datenverlust-bei-sidekick-nutzern/, zuletzt geprüft am 07.11.2013.

NIST-Computer Security Division (2011): NIST SP 800-145, The NIST Definition of Cloud Computing. Online verfügbar unter http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, zuletzt geprüft am 22.08.2013.

Ronald Eickenberg (2013): Rätselraten um Passwortsicherheit nach Evernote-Hack. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/security/meldung/Raetselraten-um-Passwortsicherheit-nach-Evernote-Hack-1817987.html, zuletzt geprüft am 12.11.2013.

Smith (2007): XII ZR 120/04. Online verfügbar unter http://www.jurpc.de/jurpc/show?id=20070001, zuletzt geprüft am 22.08.2013.

Sylvia Beckers (2013): PRISM-Überwachung: US-Cloud-Anbieter leiden unter NSA-Skandal. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/newsticker/meldung/PRISM-Ueberwachung-US-Cloud-Anbieter-leiden-unter-NSA-Skandal-1930880.html, zuletzt geprüft am 13.11.2013.

Terplan, Kornel (2011): Cloud computing. 1. Auflage. Heidelberg, Neckar: mitp/bhv.

Thörner, Oliver (2011): DC Stars eco e.V. Online verfügbar unter http://www.saas-audit.de/files/2011/03/quick-reference_de.pdf, zuletzt geprüft am 18.11.2013.

9. Stichwortverzeichnis

A

Abhängigkeit 13
Abonnement 1, 3, 4, 12
Administrationsportal 28, 29
AES-Verschlüsselung 28
Application Programming Interface 2

B

Basisschutz 18, 21, 26, 34
Bewertungs-Portale 34
Brute-Force-Angriff 18, 21
Bundesdatenschutzgesetz 17

C

CAD 4
Cloud-Computing 1
Cloud-Computing-Modelle 2
Cloud-Service 1, 2, 3, 9, 12, 13, 14, 15, 17, 25, 28, 29, 30, 34, 35, 41, 42, 43, 44, 45, 47
Cloud-Service-Provider (CSP) 1, 3, 5, 9, 17, 19, 24, 25, 27, 28, 29, 37, 41, 42, 44, 48
Community-Cloud 6, 7

D

Datenhoheit 8, 9, 17
DDoS-Angriff 19

E

Einmalcode 28
Erstinstallation 23

F

Funktionsumfangs 14

G

Gerichtsstand 27, 28, 29, 45

H

Hacker iv
HTTPS 23, 24, 25, 35
Hybrid-Cloud 5, 6

I

Infrastructure as a Service (IaaS) 2, 3, 7, 8, 9, 12, 17

Insolvenz 9, 17, 19, 20

K

Kundendienst 29

L

Lizenzen 3, 4, 12, 13, 34

M

Mandantenfähigkeit 5
Mitarbeiter-Sensibilisierung 39
Monitoring 27, 30, 35

N

NSA-Skandal iv
Nutzerverwaltung 27

P

Passwörter 17, 21, 22, 23, 29, 30
Platform as a Service (PaaS) 2, 3, 7
Private-Cloud 4
Public-Cloud 4, 5, 6, 7, 9, 11, 12, 17, 43

R

Redundanz 6
Registrierungsprozess 28, 29
Ressourcen 1, 2, 3, 5, 7, 8, 9, 12, 13, 14, 17, 18, 23, 28, 35

S

Schadsoftware 15, 18, 22
Security as a Service 30
Security-Suiten 22
Servicequalität 2, 27, 29, 42
Sicherheitsupdates 6
Sicherheitsvorfälle 15
Skalierung 15
Software as a Service (SaaS) 2, 4, 5, 7, 9, 10, 11, 14, 17, 18, 24, 27, 28, 31, 32, 37, 40, 41, 42, 44
Standards 1, 14, 20, 29, 45, 46
Storage as a Service (Cloud Storage) 1, 17, 25, 39

T

Tenant-Architektur 5

U

Übertragungsverschlüsselung 29
Übertragungsverschlüsslung 27
unbekannte Dritte 6, 15, 21, 30

V

Vendor Lock-in 20
Verbreitung von Cloud-Computing 10
Verfügbarkeit ..... iv, 13, 15, 19, 20, 27, 28, 29, 30, 36, 42, 43
Viren 18
Virtualisierung 3, 8
VPN 21, 23, 24, 25, 30, 34

W

Wartung ..... iv, 3, 4, 6, 8, 9, 12

Z

Zugangsdaten 15, 23
Zwei-Faktor-Authentifizierung 28, 30

10. Abbildungsverzeichnis

Abbildung 1: Realisierung von Cloud-Computing 2
Abbildung 2: Darstellung einer Hybrid-Cloud 6
Abbildung 3: Darstellung einer Community-Cloud 7
Abbildung 4: Verbreitung von Cloud-Computing im Handwerk 11
Abbildung 5: Rechte-Management bei Owncloud 26
Abbildung 6: Weka Handwerksbüro 31
Abbildung 7: Lexoffice von Lexware 33
Abbildung 8: Erkennbare Passwortsicherheit 34

ISBN: 978-3-944916-08-8