:get know howww
UBIT Steiermark

Bildungsthema

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

Themenexperten:

IT Security ExpertsGroup der WKÖ – www.itsecurityexperts.at

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

Harald Wenisch,
Wenisch Consulting e.U.

Co-Autoren dieses Kapitels:

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

HansChristian Einfalt - sevian7 IT development GmbH

Florian Brunner, BSc - Holistic Security Consulting GmbH

Christian Gegenhuber, edv.service.gegenhuber OG

Erik Rusek, BSc – Holistic Security Consulting GmbH

Siegfried Schauer – IKARUS Security Software GmbH

DI Martin Schober – MSC martin.schober

März 2014

Inhaltsverzeichnis

1 KAPITEL 2 – Wege in die Cloud

Einleitung

„Denn es ist zuletzt doch nur der Geist,
der jede Technik lebendig macht!" (Johann Wolfgang von Goethe)

Das Zitat von Goethe ist signifikant für eine Entscheidung zur Nutzung einer Cloud-Lösung. Wie die Technik der Cloud genutzt wird und welchen Vorteil sie einem Unternehmen bringen kann, liegt in der Arbeitsweise des Menschen, der sie nutzt. Die Grundidee der Cloud wurde bereits im 1. Kapitel angeführt. Der Zugriff von überall auf die eigenen Daten und Programme zur Schaffung einer Unabhängigkeit von eigener Infrastruktur. Ganz so weit sind wir noch nicht, da sie nach wie vor auf ein Endgerät in vorm eines Notebooks, PCs oder Tabletts angewiesen sind, dennoch ist es bereits heute möglich, ohne eigene Server-Infrastruktur das Auslangen zu finden.

Kapitel 2 behandelt die unterschiedlichen Wege in die Cloud und befasst sich vor allem damit, wie Sie die Cloud nutzen können. Das letzte Kapitel der Reihe wird sich mit dem Ausstieg aus der Cloud befassen. Da die Gründe hierfür sehr ähnlich zu jenen sind, die auch zu einer Entscheidung führen überhaupt nicht in die Cloud zu gehen, wird dieser Punkt zwar als „Weg“ angeführt, aber nicht näher beschrieben, da dies in Kapitel 3 folgt.

Cloud-Anbieter

Für dieses Kapitel möchten wir insbesonders auf die Checkliste der WKÖ für die Auswahl von Cloud-Anbietern hinweisen. Sie finden diese unter WKÖ Der Cloud Vertrag[1].

Unabhängig davon, für welche Cloud-Lösung Sie sich entscheiden, ist ein Grundbestandteil die Wahl des Anbieters. In diesem Kapitel lernen Sie unterschiedliche Cloud-Anbieter und verschiedene Kriterien kennen, mit denen Sie die unterschiedlichen Anbieter vergleichen können - zuvor allerdings einige Worte zur Cloud selbst und zu den Unterschieden einer Cloud-Lösung.

Grundsätzlich besteht jedes IT-System aus drei Teilen: der Hardware, des Netzwerks und der Software. Die Hardware (Computer, Server, Festplatten) sind mit einem Netzwerk verbunden (Intranet, Extranet, Internet) und die Software läuft auf dieser Hardware und in diesem Netzwerk.

Jetzt kann man als Cloud-Lösung alle drei Teile in eine Wolke schieben, nur die Hardware oder nur die Software oder nur das Netzwerk - oder zwei von diesen Teilen. Jedes Szenario hat Vor- und Nachteile und oft auch einen anderen Namen.

Wird nur die Hardware in eine Cloud gestellt, beziehungsweise die Hardware via Cloud verwendet, kann darauf die eigene Software und ggf. via VPN auch ein eigenes Netzwerk verwendet werden – es entstehen keine Hardware-Anschaffungskosten und auch kein Service rundherum. Das alles übernimmt der Hoster – in diesem Fall sprechen wir z.B. von dedizierten Servern von 1und1.de.

Wird nur die Software in eine Cloud „geschoben“, dann läuft diese natürlich auch auf einem Server, allerdings hat der Kunde nur Zugriff auf den Software-Teil und kann keine eigenen Programme installieren. Der Vorteil dieser Lösung ist wieder im geringen Administrationsaufwand zu finden. Alle Updates, Upgrades, zusätzliche Installationen, Fehlersuche u.dgl. werden vom Hoster übernommen. Ein Beispiel wäre das Office 365 von Microsoft.

Nur das Netzwerk in eine Cloud zu stellen ist auch möglich. Das bedeutet, dass die Hardware (Server) und die Software die darauf läuft beim Kunden stehen und Mitarbeiter via eines Cloud-Netzwerks darauf zugreifen. Das kann via Remote-Desktop oder generell via

[1] https://www.wko.at/Content.Node/branchen/oe/sparte_iuc/Unternehmensberatung-und-Informationstechnologie/DER_CLOUD_VERTRAG_3.pdf

VPN erfolgen. Dann erfolgt der Zugriff auf die eigene Infrastruktur über Fremdanbieter und dessen Servern. Diese sorgen für korrekte Firewalls, Verschlüsselungen und Protokolle. Ein Beispiel dafür ist die Firma Fastviewer.

Anhand dieser Beispiele lässt sich erkennen, dass auch Hybrid-Lösungen möglich sind. Je nach Anwenderfall macht das eine oder andere Sinn. Meist wird der Faktor in eine Cloud gestellt, der entweder sehr teuer beziehungsweise aufwendig zu administrieren ist oder der keine Firmen-Geheimnisse oder Patente birgt.

Um zwei Beispiele zu nennen:

Eine Tischlerei mit speziellen Fertigungsmethoden wird ihre fertigen 3D-Entwürfe gerne bei sich auf einem Server gespeichert haben, allerdings kann der Rechenaufwand für die 3D-Designs inklusive der Software dazu leicht einer Cloud in Verantwortung übergeben werden. Immobilien-Makler werden ihren Kundenstamm ungern in einer Cloud sehen, aber die Fotos von Immobilien sind schon aufgrund der Größe, Menge und der Veröffentlichung via Internet in einer Cloud gut aufgehoben.

Auch für die **Art der Nutzung** gibt es unterschiedliche Begriffe, die wir hier nochmals kurz wiederholen. Sie finden diese auch in Kapitel 1.

- IaaS – Infrastructure as a Service – die Grundstruktur

Sind virtualisierten Computerhardware-Ressourcen wie Rechner, Netzwerke und Speicher. Mit IaaS gestalten sich Nutzer frei ihre eigenen virtuellen Computer-Cluster und sind daher für die Auswahl, die Installation, den Betrieb und das Funktionieren ihrer Software selbst verantwortlich.

- PaaS – Platform as a Service – oft auch als Middleware bezeichnet

Rechnerwolken bieten Nutzungszugang von Programmierungs- oder Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten. Mit PaaS entwickeln Nutzer ihre eigenen Software-Anwendungen oder lassen diese hier ausführen, innerhalb einer Softwareumgebung, die vom Dienstanbieter (Service Provider) bereitgestellt und unterhalten wird.

- SaaS – Software as a Service – die Spitze der Services

Rechnerwolken bieten Nutzungszugang von Software-Sammlungen und Anwendungsprogrammen. SaaS Dienste-Anbieter offerieren spezielle Auswahlen von

Software, die auf deren Infrastruktur läuft. SaaS wird auch als Software on Demand (Software bei Bedarf) bezeichnet.

Auswahl eines Cloud-Anbieters

Die Auswahl eines Cloud-Anbieters ist nicht so trivial, wie es auf den ersten Blick scheint. Ohne exakte Kenntnisse der Anforderungen ist keine sinnvolle Auswahl möglich.

Darum lassen Sie uns zuerst einen Blick auf die Einsatzarten einer Cloud-Lösung werfen (Punkt 1); danach schauen wir uns die Datensicherheit (Punkt 2) und zum Schluss die Eigenschaften und Kriterien (Punkt 3) etwas genauer an.

Einsatzarten von Cloud-Lösungen:

Wir haben in der Einleitung ja schon über IT-Systeme und deren Teile gesprochen, die sich in eine Cloud verschieben lassen.

Cloud-Lösungen selbst können jetzt nochmal nach dem Speicherort der Daten in drei große Gruppen gegliedert werden:

- **Reine Cloud-Lösung** - alle Daten liegen nur in der Cloud, es existiert kein Speicher für Daten im Unternehmen.

Vorteile: keine Kosten für die Hardware (Storage), keine Stromkosten, keine Administrator Kosten und die Daten sind von überall immer abrufbar.

Nachteile: keine rasche „Verfügungsgewalt“ über die Daten, Datenklau wird nicht bemerkt (da keine eigene Aufsicht), im Fehlerfall kein Zugriff, ungutes Gefühl da unbekannt ist, wo genau die Daten liegen, wie der Admin damit umgeht usw.

- **Hybridlösung:** Daten liegen in der Cloud aber auch in der Firma. Hier gibt es 2 Szenarien:
  1. alle Daten liegen in der Cloud und dieselben Daten liegen auch beim Unternehmen. Das ist zB bei jedem hosted Exchange der Fall. Achtung: Das hat mit einer Backup-Lösung (Datensicherung) nichts zu tun!

Vorteile: einfache Verteilung der Daten via Cloud, Sicherung der Daten im eigenen Netzwerk, Admin-Aufwand gering, da nur Sicherung eine Rolle spielt. Schneller Zugriff auf die Daten, auch im Fehlerfall Zugriff möglich.

Nachteile: Datensicherheit wie bei einer reinen Cloud-Lösung, Datendiebstahl wird auch nicht bemerkt, es entstehen Kosten für eine Datensicherung, obwohl der Hoster auch dafür sorgt – Doppellösung, die kein „Mehr“ an Sicherheit bringt.

2. zweites Szenario: Die wichtigen/geheimen Daten liegen im Unternehmen, die anderen Daten zwecks Verteilung in der Cloud.

Vorteile: die Datensicherheit ist höher, Verfügungsgewalt über die Daten vorhanden, Verteilung möglich, Datenklau beziehungsweise der Versuch wird bemerkt. Nachteile: Administrationsaufwand und das Managen welche Daten gehört zu welcher Klassifizierung, Verteilung komplex.

- **Backup-Cloud:** Alle Daten liegen im Unternehmen, nur die Datensicherung wird in die Cloud gespielt

Vorteile: Daten können verschlüsselt übertragen und auch verschlüsselt gespeichert werden, einfache Datensicherung ohne Zutun des Benutzers, die Lösung ist rasch implementiert und einfach.

Nachteile: Bei großen Datenmengen hoher Bandbreitenbedarf, Wiederherstellung im Fehlerfall kann sehr lange dauern (bei großen Images).

Datensicherheit:

Bevor wir über die Datensicherheit sprechen müssen wir zuerst die Daten klassifizieren. Das bedeutet, eine Einteilung machen: was sind Daten, welche davon sind kundenbezogen, welche geheime / interne Daten, welche davon sind besonders schützenswert (Patente, Rezepte, Kontostände, usw.). Nach der Klassifizierung stellt sich die Frage, welche Daten sollen wie geschützt / gespeichert werden (inkl. Zugriffsberechtigungen) und erst danach kann eine Entscheidung getroffen werden, wo die Daten liegen sollen bzw. dürfen. Es spielt in der Cloud eine große Rolle, wo der Server steht auf dem die Daten gespeichert werden, da das Gesetz des Staates gilt, in dem sich der Server befindet.

Unter Datensicherheit wird definiert, wie und vor wem Daten geschützt werden müssen, wie und wie lange sie aufbewahrt gehören, wer alles darauf Zugriff hat, wo und wie sie gespeichert gehören und wann und von wem sie gelöscht werden müssen / dürfen. Weiters fällt unter Datensicherheit wie gelöschte Datenträger entsorgt werden und was passiert bei einem Datenklau beziehungsweise bei dem Versuch eines Diebstahls (wer wird verständigt, To-Do Liste u.dgl.).

All diese Fragestellungen sind wichtig, um entscheiden zu können, welchen Cloud-Anbieter Sie wählen und ob Sie sich bei Datenspeicherung überhaupt für eine Cloud-Lösung entscheiden sollen. Es gibt auch die Möglichkeiten nur die Infrastrukturen zum Rechnen oder Versenden von Daten via Cloud zu nutzen ohne die Speicherung von Daten – ein Punkt der oft vergessen wird.

Zuletzt ist noch entscheidend wo der Server eines Hosters steht, in welchem Staat und wo die Firma des Hosters ihren Sitz hat. Strafrechtlich ist es relevant für Klagen bei Datendiebstall /Verlust, bei Urheberrechtsverletzungen oder bei zivilrechtliche Klagen, wo der Anbieter (Hoster) niedergelassen ist und wo er die Leistung erbringt. Da hat jeder Staat seine eigenen Gesetze und viele Staaten nehmen es mit der Datensicherheit bzw. dem Datenschutz nicht sehr genau – das gilt z.B. besonders für Amerika oder China. Andere wiederrum haben ein striktes Datenschutzgesetz – wie Österreich oder etwas eingeschränkt auch Deutschland.

Die Eigenschaften von Cloud-Systemen

Wir Experten werden oft gefragt, welcher Cloud-Anbieter der beste beziehungsweise welcher zu empfehlen ist. Darauf kann pauschal keine Antwort gegeben werden. Zu unterschiedlich sind einerseits die Anforderungen des Kunden, andererseits die Leistungen der Cloud-Anbieter.
Lassen Sie uns kurz einen Blick auf die wichtigsten Kriterien der einzelnen Leistungen werfen. Damit kann rasch ein eigenes Wunsch-Profil erstellt werden um den richtigen Anbieter zu finden beziehungsweise die Suche gut einzugrenzen. Somit wird nicht nur der Preis als Hauptaugenmerk verwendet. Der Preis sollte als eines der letzten und unwichtigsten Kriterien gelten, da gerade in der EDV die Datensicherheit, die Zugriffskontrollen und Bandbreiten, sowie Standorte in „sicheren“ Staaten hohe Kosten verursachen können - und was helfen Ihnen ein paar hundert gesparte Euro im Monat wenn Ihre Daten weg sind und ein anderer sich ihrer erfreut.

Eigenschaften im Überblick:

- **Service Levels**
  Gibt es verschiedene Service-Levels, wenn ja welche und was kosten diese? Wie ist die Verfügbarkeit der Server, was geschieht im Fehlerfall? Werde ich benachrichtigt, wenn ja wie? Was passiert bei Wartungen usw.
  Gerade in diesem Punkt trennt sich „Spreu von Weizen“ und kleine Provider haben da oft die Nase vorn, was sich natürlich auch im Preis widerspiegelt.

- **Sicherheitsstandards**
  Welche Sicherheitsstandards gelten für den Zutritt zum Server? Kann da jeder hin oder ist das ein geschützter Bereich. Wenn geschützt, wie? Rund um die Uhr? Was geschieht bei einem Stromausfall? Gibt es USVs (Stromversorgungen)? Wie lange halten diese? Sind Naturkatastrophen berücksichtigt?
  Hochwasser, Sturm? Was passiert wenn ein Server defekt ist? Wird eine Datensicherung gemacht, wenn ja wie oft und wann?
  Diese Standards sind wichtig. Viele Provider sind in einem Rechenzentrum untergebracht, was teurer ist als in einem Keller den Server stehen zu haben, aber um Welten sicherer.

- **Verschlüsselungen**
  Bietet der Cloud-Anbieter Verschlüsselungen an? Nur am Server (am Speicherplatz) oder schon am Weg dorthin? (Verbindungssicherheit). Wenn ja, welche? Welchen Standard und wie groß ist die Schlüssellänge?
  Dieser Punkt ist relevant, wenn geheime oder firmenrelevante Daten gespeichert werden – am Weg via Internet kann leicht mitgelesen werden.

- **Serverstandort**
  Wo steht der Server? Das ist für den Datenschutz - wie weiter oben im Text schon diskutiert - rechtlich relevant und auch wichtig für Klagen und Vergehen. Für Backup-Lösungen kann im Fehlerfall oft auch ein manuelles Backup zur Wiederherstellung angefordert werden. Da ist geographische Nähe von Vorteil.

- **Firmensitz**
  Der nächste relevante Punkt für Datenschutz und Datensicherheit. Wurde bereits abgehandelt – wird oft unterschätzt. Stichwort: NSA, Patriot Act und Industriespionage.

- **Erreichbarkeit / Hotline**
  Gibt es eine Hotline oder andere Wege, den Anbieter zu kontaktieren? Wie sind die Öffnungszeiten? Was passiert im Fehlerfall? Ruft mich der Provider zurück?
  Wichtig deshalb, weil es bei Kommunikation nur via e-mail oder chat gerade bei Netzwerkfehlern zu Störungen kommen kann.

- **Preis-Leistungsverhältnis (EUR/GB)**
  Der Ordnung halber wurde dieser Punkt eingefügt. Wichtig sind andere Themen, erst bei vollständiger Gleichheit aller anderen Kriterien ist dieser Punkt relevant. Leider lassen sich zu viele durch auf den ersten Blick günstige Preise pro GB ablenken. Eines sollte jedem

Kunden klar sein: Qualität kostet Geld – gerade im Cloud-Bereich können die Anschaffungskosten für qualitative Hard- und Software sehr hoch sein.

- **Zugriffsmöglichkeiten**
  Welche Zugriffsmöglichkeiten gibt es für meine Daten? Ein Programm das installiert werden muss? Für welches System funktioniert das? Windows, Apple, Linux? Was ist mit Smartphones, Tablets? Gibt es einen Admin-Zugang? Kann ich Zugriffe beschränken? Wie bequem ist die Software? Brauche ich eine Einschulung dafür? Was kostet das Programm? Was die Einschulung? Bitte beachten Sie auch, dass mannigfaltige Möglichkeiten auch viele Sicherheitsfragen aufwerfen!

- **Schnittstellen**
  Das Thema Schnittstellen wird oft vernachlässigt. Dabei ist es essentiell, mittels welchem Protokoll und über welche Schnittstelle kommuniziert wird. Dieser Port muss in einer Firewall freigeschaltet werden, das Protokoll muss zugelassen werden und so sicher und gut das Protokoll ist, so gut und sicher sind Ihre Daten gespeichert. Schnittstellen spielen auch beim Transfer größerer Datenmengen eine wichtige Rolle. Details dazu sagt Ihnen gerne Ihr IT-Berater.

- **Bandbreite / Anbindung**
  Je größer die Bandbreite umso mehr Daten können innerhalb einer gewissen Zeit übertragen werden – soweit zur Theorie.
  In der Praxis sieht das ganz anders aus: wichtig ist nicht die Bandbreite Ihres Cloud-Anbieters, sondern im ersten Schritt Ihre eigene! Dabei spielt es eine große Rolle, ob Sie eine synchrone Leitung haben (Up- und Download sind gleich schnell) oder eine asynchrone Anbindung (schneller Down- langsamer Upload). Bei großen Datenmengen (z. Bsp. Backup-Lösungen) kann schnell einmal das Netzwerk zum Erliegen kommen, da kann Ihnen dann ein guter Cloud-Anbieter mehrere Lösungen anbieten, beziehungsweise Sie technisch beraten.
  Grundsätzlich besitzen fast alle Anbieter von Cloud-Lösungen eine ordentliche Anbindung – vor allem in Österreich sind die Flaschenhälse immer bei den Kunden zu suchen, da unsere Netzwerk-Infrastruktur vor allem in ländlichen Bereichen oft der Zeit hinterherhinkt.

- **Datensynchronisation**
  Der letzte technische Punkt hängt mit der Bandbreite zusammen: die Synchronisation. Was für Sync-Arten bietet mir mein Cloud-Anbieter an? Damit kann ich eine geringe Bandbreite kaschieren (in Maßen) und trotzdem mein Backup machen, oder meine Daten up-to-date halten. Allerdings sind da Grenzen gesetzt. Untertags wird aufgrund des Tagesgeschäfts Bandbreite zum Arbeiten benötigt, da muss die Synchronisation warten, wenn die Bandbreite zu gering ist oder die Datenmenge zu groß ist – gerade diese Fragestellung ist enorm wichtig und eine Entscheidungsgrundlage für und gegen eine speziellen Cloud-Lösung.

- **Vertragslaufzeiten**
  Ein wichtiges Thema ist, wie lange Sie sich an einen Provider binden müssen und was Sie im Gegenzug erhalten. Rabatt für 2 Jahre oder mehr Bandbreite oder Speicherplatz? Oder bevorzugen Sie einen rasch möglichen Ausstieg?

- **Kündigungsbedingungen**
  Passend zum oberen Punkt ergibt sich die Frage „Wie kann ich kündigen?“. Was müssen Sie tun, wie aufwändig ist das und was passiert mit Ihren Daten nach Ende der Vertragslaufzeit?

Handlungsleitfaden

Hier wird versucht, einen kurzen Handlungsleitfaden zu geben.

Wann geht ein Unternehmen in die Cloud und warum

Unabhängig von der Unternehmensgröße und Branche können Cloud-Dienste attraktiv sein. Zu Beginn stellt sich die Frage, welche Services und Anwendungen Ihres Unternehmens sinnvoll in die Cloud verlagert werden können.

Einer der ältesten Cloud-Dienste ist das E-Mailpostfach beim Provider. Dieser Dienst existierte bereits schon lange vor dem Begriff „Cloud“ in Bezug auf IT. Auch der Webspace beim Webhoster ist ein klassischer Dienst in der Wolke. Cloud-Dienste kennt man auch als IaaS (Infastructure as a Service), PaaS (Platform as a Service) oder SaaS (Software as a Service).

Enterprise Dienste für Jedermann

Kleinen und mittelständischen Unternehmen wird durch Cloud-Services oft der Zugang zu Software und Kommunikationslösungen erleichtert, welche in Vergangenheit nur für große Unternehmen leistbar waren, z.B. Termin und Kontaktsynchronisation in Echtzeit auf allen Geräten.

Verschlankung der IT-Infrastruktur

Durch das Auslagern von Daten und Diensten in die Cloud kann die lokale IT-Infrastruktur reduziert werden. Das bedeutet weniger Investitionskosten und weniger Wartungsaufwand.

Verfügbarkeit und Sicherheit

Auch beim Thema Verfügbarkeit und Sicherheit können Cloud-Services den klassischen Inhouse-Lösungen überlegen sein. Viele Anbieter halten hochverfügbare Infrastrukturen und aktuelle Sicherheitstechnologien zum sicheren Bereitstellen der angebotenen Dienste bereit. Allerdings sollte beachtet werden, dass kein Zugriff auf die Daten und Dienste in der Cloud mehr möglich ist wenn Ihre Internetanbindung ausfällt - außer die Cloud-Dienste sind im lokalen Netzwerk verfügbar (nur mit einer Private Cloud realisierbar).

Bei Onlineplattformen (z.B. Webshops, Foren …) steht die Verfügbarkeit an erster Stelle, daher kann es sinnvoll sein diese Anwendungen in die Cloud auszulagern.

Teamwork

Die Zusammenarbeit zwischen einzelnen Mitarbeiter, Freelancern, Kunden oder Lieferanten kann durch Cloud-Dienste wesentlich effizienter funktionieren. Zum Beispiel können Sie ihrem Lohnfertiger Pläne direkt in der Cloud zur Verfügung stellen – je nach Anbieter auch mit Versionierung und einem Änderungsverlauf.

Dynamische Kapazitäten (Pay per use)

Cloud-Lösungen bieten oft die Möglichkeit, die Benutzeranzahl, Rechenleistung oder Speicherkapazität dynamisch zu verändern. Damit ist es einfach möglich in Spitzenzeiten die benötigten Ressourcen zu erhöhen bzw. wieder zu verringern wenn der Bedarf sinkt. (Per User / Transaktaktion / Volumen / Zeit / Transfer)

Selfservice

Ein weiterer Vorteil der Cloud kann das Selfservice sein. Dabei kann sich der Kunde selbst Ressourcen aus dem Pool des Cloud-Providers bedienen. Sprich der Anbieter stellt Ihnen eine Oberfläche zur Verfügung, mit der Sie die erforderlichen Ressourcen an Hardware (Speicher, Prozessor, RAM) aber auch an Diensten wie Mail-Postfächer, Benutzer-Acounts odgl. selbst anlegen können. So können rasch und einfach die benötigten Kapazitäten zur Verfügung gestellt werden. Zumeist basieren diese Systeme auf „virtualisierten“ Umgebungen. Es wird Ihnen eine virtuelle Maschine zur Verfügung gestellt, die Sie nach Ihren Anforderungen erweitern können. Hierbei sind aber immer Sie für die vorgenommenen Einstellungen auch verantwortlich.

Welche Vorbereitungen sind zu treffen

Um Cloud Computing bestmöglich in die bestehende Infrastruktur zu integrieren sollten einige Vorbereitungen getroffen werden.

Was soll in die Cloud verlagert werden

Zu Beginn stellt sich die Frage, welche Dienste und Ressourcen in die Wolke verlagert werden sollen (die gesamte Infrastruktur, Daten, einzelne Dienste, Backup usw.)

Dadurch beantwortet sich zum Teil schon die Frage, welches Cloud-Model (Public-, Private- oder Hybrid Cloud) sinnvoll sein kann.

Klassifizierung der Daten

Sollten Sie Ihre Daten noch nicht klassifiziert haben ist jetzt der geeignete Zeitpunkt dafür. Die Klassifizierung ist notwendig, um die rechtlichen Aspekte und interne Richtlinien einhalten zu können. Beispiel: Personenbezogene Daten sind anders zu handhaben als technische Dokumente oder betriebswirtschaftliche Daten. Dabei muss nicht unbedingt die Wichtigkeit der Daten im Vordergrund stehen.

Details zu Datenklassen: https://www.sicherheitshandbuch.gv.at

Kosten und Wirtschaftlichkeit

Ein nicht unwesentlicher Faktor sind auch die Kosten. Generell lässt sich keine Aussage machen, ob Cloudcomputing günstiger ist als eine konventionelle IT-Infrastruktur. Dies sollte von Fall zu Fall neu verglichen und bewertet werden.

Vorhandene Hard- und Software

Auch für Cloud Computing sind PCs und Internetverbindung notwendig. Es empfiehlt sich vorab zu überprüfen, ob mit der vorhandenen Hard- und Software der Zugriff auf die Cloud-Dienste möglich ist. Überprüfen Sie auch, ob die Versionen zueinander auch kompatibel sind.

Lokale Internetanbindung

Damit der Zugriff auf Cloud-Dienste möglichst reibungslos funktioniert sollte die lokale Internetverbindung stabil und ausreichend schnell sein. Um bei einem Ausfall des lokalen Internetanschlusses schnellst möglich weiterarbeiten zu können empfiehlt es sich, die SLAs beim Internetprovider zu überprüfen und ggf. einen alternativen Internetzugang anzuschaffen.

Welche Abklärungen sind erforderlich

Bevor die Entscheidung auf einen Cloud-Serviceanbieter fällt, sollten einige Punkte im Vorhinein abgeklärt werden. Beachten Sie: ein nachträglicher Wechsel eines Anbieters ist oft aus organisatorischen Gründen nur sehr schwer möglich und kann hohe Kosten verursachen.

Kundenspezifische Anpassungen

Speziell bei Kaufmännischer Software sind manchmal kundenspezifische Anpassungen notwendig. Sind diese Anpassungen (z.B. von Formularen und Auswertungen) möglich?

Schnittstellen zwischen Anwendungen

Viele lokale Programme bieten und nutzen Schnittstellen. Wenn solche Programme in die Cloud verlagert werden sollen, sollte auch abgeklärt werden ob die Schnittstellen weiterverwendet werden können und welcher Aufwand dafür nötig ist.

Backup und Recovery

Wer übernimmt die Verantwortung für die Datensicherung? Es bedeutet nicht automatisch, dass der Cloud-Anbieter periodisch Ihre Daten sichert!

Wie schnell können Ihre Daten im Notfall wiederhergestellt werden und ist es möglich, einzelne Datensätzen wiederherzustellen? Dabei sollte auch beachtet werden, ob und wie die Datenwiederherstellung nach unbeabsichtigter Löschung durchgeführt werden kann.

Softwareupdates

Je nach Anwendung und Anbieter erscheinen in unterschiedlichen Intervallen neue Versionen auf den Markt. Hier ist darauf zu achten, wie der Anbieter der Cloud-Lösung mit Updates und Upgrades umgeht. Ein Update ist zumeist eine Verbesserung einer Software innerhalb der bestehenden Versionsnummer. Sie kennen dies von Windows 7 Updates. Ein Upgrade ist der Sprung auf die nächste Version. Beispielsweise von Windows 7 auf Windows 8. Die Cloud-Anbieter behandeln diese Thematik unterschiedlich. Einige führen die Updates und Upgrades automatisch im Hintergrund für Sie durch, andere zwar die Updates aber die Upgrades nur gegen Aufpreis. Egal welche Variante, wichtig ist für Sie, dass Sie informiert werden, WANN und WAS verändert wird. Es kann nach einem Update, aber vor allem nach einem Upgrade, vorkommen, dass eine von Ihnen angepasste Lösung nicht mehr wie erwartet funktioniert, ein Makro in einem Dokument nicht mehr so abläuft, wie Sie es benötigen würden.

Datensicherheit und Datenschutz

Welche Maßnahmen unternimmt der Cloud-Serviceanbieter um Daten vor Diebstahl und unautorisierten Zugriff zu schützen? Es sollte der Zugriff nur über verschlüsselte Verbindungen erfolgen können und die Daten selbst sollten Verschlüsselt abgelegt werden.

Der geografische Serverstandort und die Unternehmenszugehörigkeit des Anbieters sind ebenfalls ein Punkt, den Sie in die Entscheidungsfindung mit einbeziehen sollten. Ein wichtiger Standard zur Auswahl von Rechenzentren kann ISO 27001 sein. Der Standard berücksichtigt jedoch nicht die Sicherheit der Anwendung, sondern nur das Rechenzentrum.

Verfügbarkeit

Die Verfügbarkeit von Cloud-Diensten wird in den SLA‘s [Service-Level-Agreement] angegeben. Dabei ist darauf zu achten, dass die gebotene Verfügbarkeit den Anforderungen entspricht. So bedeutet beispielsweise eine Verfügbarkeit von 99 Prozent, dass der Dienst 87,6 Stunden im Jahr ausfallen kann, ohne dass der Anbieter zu Schadensersatzzahlungen verpflichtet ist.

Vertragsdetails

Abschließend sollten Vertragsdetails, wie Bindungsfristen, Überschreiten von inkludierten Transfervolumen oder Paketupgrades berücksichtigt werden.

Wo und Wie kann mir mein IT-Dienstleister helfen

Um ein Cloud-Projekt erfolgreich und ohne größere Pannen durchführen zu können ist es sinnvoll, einen IT-Dienstleister Ihres Vertrauens einzubinden.

IST Analyse

Bestandsaufnahme der bestehenden Infrastruktur. Klassifizieren der Daten und Dienste. Dokumentieren von Schnittstellen zwischen Applikationen

Präzisieren von Zielen

Die Ziele, die mit dem Einstieg in die Cloud erreicht werden sollen, sollten im Vorfeld definiert und ggf. in einem Lastenheft festgehalten werden.

Über Stolpersteine aufklären

Aufklärung über rechtliche-, organisatorische- und technische Risiken und wie diese erfolgreich bewältigt werden können.

Planen der Abläufe

Erstellen eines Zeitplans, Notwendige Schritte für Export/Import und Datenübernahme

Lösungen vergleichen

Unterstützung bei der Providerauswahl durch das Vergleichen von technischen Details und Vertragsbedingungen

Inbetriebnahme und Konfiguration

Einrichtung des Cloud-Dienstes, Anlegen der Benutzerkonten, Datenübernahme, Anpassungen, Backup …

Policy Management und Qualitätsmanagement

Erstellen und Kontrollieren von Richtlinien.

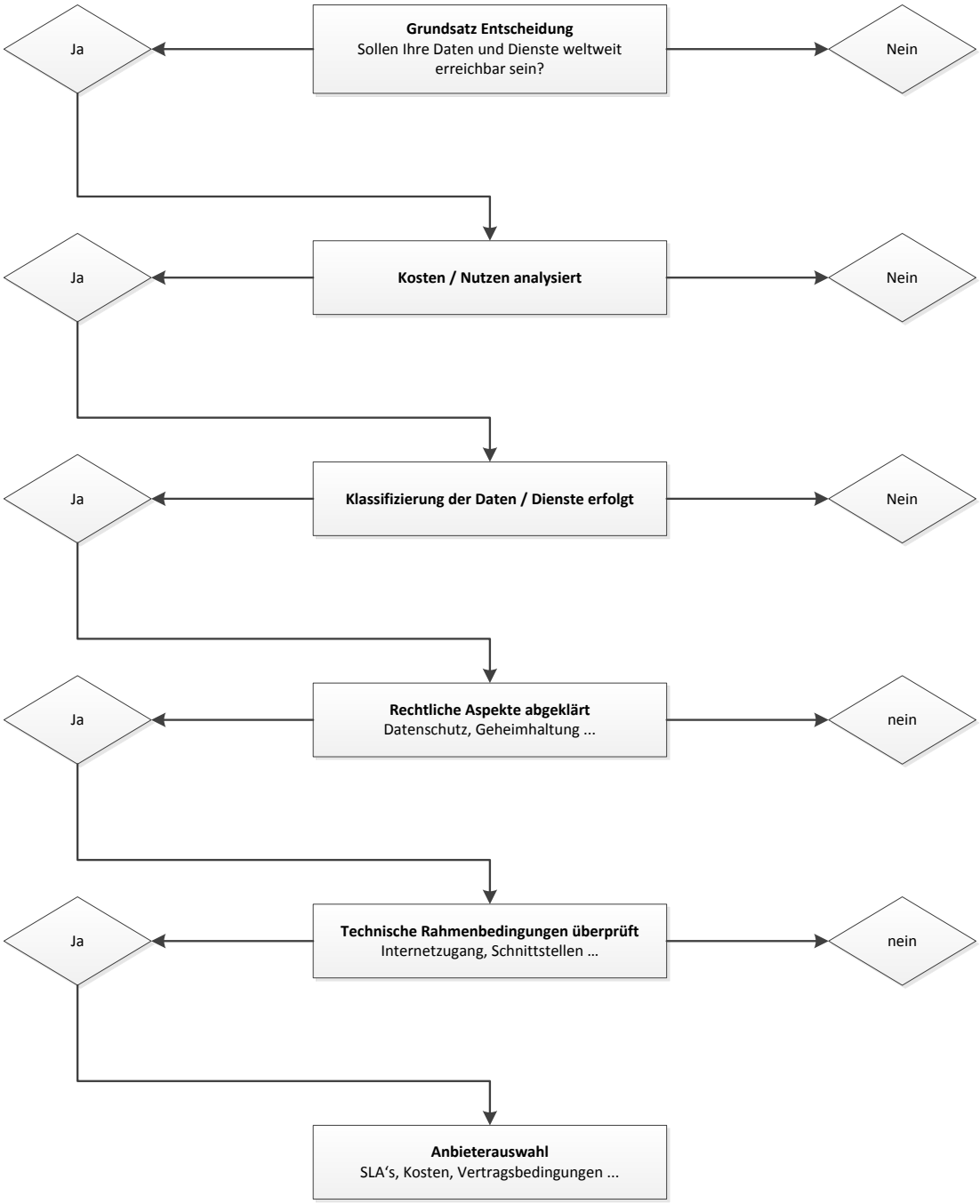
Dokumentieren

Erstellung einer Projektdokumentation um diverse Schritte und Einstellungen nachvollziehen zu können.

Benutzer / Administratoren schulen

Einschulung der Benutzer um das „neue System“ effektiv nutzen zu können. Administrative Benutzer über die Möglichkeiten / Funktionen des Selfserviceportal aufklären.

Der Weg in die Cloud



Informationssicherheit in der Cloud

Datenzugriffe

Rechte- und Identitätsmanagement

Um Zugriffe in die Cloud und auf die Ressourcen innerhalb der Cloud zu steuern und zu kontrollieren, ist es notwendig ein entsprechendes Rechte- und Identitätsmanagement zu etablieren, vgl. (Cordial, 2011) (Kuppinger, 2012). Basierend auf dieser Notwendigkeit entstehen zwei grundsätzliche Anforderungen:

- Das Unternehmen muss beim Umstieg auf Cloud-Systeme ein Rechte- und Identitätsmanagementkonzept erarbeiten bzw. das bestehende Konzept anpassen.
- Der Cloud-Provider muss entsprechende Möglichkeiten für die Umsetzung des Konzeptes bieten.

Bei existierenden lokalen Zugriffskonzepten bieten verschiedene Cloud-Provider die Möglichkeit die bestehenden Konzepte direkt an die Systeme des Cloud-Providers anzubinden. Dies spart beim Einsatz Zeit und Änderungen werden automatisch mit der Cloud synchronisiert.

In weiterer Folge ist der Cloud-Provider auch in der Pflicht, eine transparente Aufschlüsselung zwischen Zugriffen der Kunden und jenen der Administratoren des Unternehmens zur anzufertigen und zur Verfügung zu stellen.

Benutzer- und Rollenkonzept

Unabhängig ob es sich beim auszulagernden Dienst um einfachen Datenaustausch zwischen Abteilungen, Niederlassungen oder mit Partnerunternehmen handelt, es wird empfohlen ein entsprechendes Benutzer- und Rollenkonzept anzuwenden. Damit wird sichergestellt, dass nur bestimmte Personen bzw. Rollen auf definierte Daten zugreifen können und dieser Zugriff wiederum protokolliert und kontrolliert werden kann.

Es ist wesentlich dabei darauf zu achten, dass das Konzept in regelmäßigen Abständen auf Aktualität geprüft und gegebenenfalls angepasst wird. Auch hier ist darauf zu achten, dass lokal bereits existierende Konzepte bei verschiedenen Cloud-Anbietern automatisch angebunden werden können und so die Verwaltung der Regelungen vereinfachen.

Access-Control und Authentifizierungsmechanismen

Der Cloud-Provider muss Mechanismen zur Zugriffskontrolle und –Steuerung der Ressourcen in der Cloud zur Verfügung stellen.

Konkret bedeutet dies einerseits, dass das Unternehmen bei der Verwendung von Cloud-Services jederzeit in der Lage sein muss Zugriffe zu aktivieren und zu deaktivieren bzw. temporäre Zugriffe mit Benutzerbindung zu vergeben. In weiterer Folge müssen die jeweiligen Zugriffe und Zugriffsversuche protokolliert und abrufbar sein. Die Protokollierung inkludiert Maßnahmen die im Falle mehrfacher ungültiger Zugriffe, wie zum Beispiel die Sperrung des Kontos, ergriffen werden können.

Die Art des Authentifizierungsmechanismus ist zu berücksichtigen, insbesondere welche Authentifizierungsverfahren und –Merkmale eingesetzt werden und ob beispielsweise Mehr-Faktor-Authentifizierung möglich ist.

Ein weiterer Aspekt ist die Passwort-Komplexität, also die Länge und die erlaubten Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen) die das Passwort beinhalten kann. Speziell bei einfacher Benutzer-Passwort-Authentifizierung ist dieses Sicherheitsmerkmal ausschlaggebend für die Zugriffssicherheit auf die Ressourcen innerhalb der Cloud. Bei der Auswahl des Cloud-Anbieters ist daher besonders darauf zu achten, dass die Passwort-Komplexität durch diesen nicht limitiert wird.

Weitere Sicherheit verschafft die Anwendung von Mehr-Faktor-Authentifizierung, eine Kombination von Authentifizierungsmethoden. Ein mögliches Szenario wäre die Verbindung von Benutzer-Passwort Authentifizierung mit so genannten Hardware-Tokens.

Ein weiterer wesentlicher Punkt ist die Festlegung bzw. Übermittlung der Zugangsdaten an den Benutzer. Denkbare Varianten wären hier die Auswahl der Authentifizierungsdaten direkt auf der Plattform bzw. bei der Verwendung von Einmal-Passwörtern eine getrennte Übertragung von URL und Passwort per E-Mail bzw. SMS.

Datenverwaltung

Backup- und Restorefunktionalität

Datenverlust, defekte Hardware und zerstörte Daten sind Themen mit denen sich KMUs ebenfalls auseinandersetzen müssen. Aus diesem Grund ist eine angemessene Backup-Strategie betreffend der unternehmensinternen Daten unumgänglich. In der Regel bieten die

meisten Cloud-Provider entsprechende Backup-Mechanismen an. Bei der Verwendung dieser Services gibt es allerdings verschiedene Aspekte zu beachten.

In erster Linie muss die Wiederherstellbarkeit der Daten geprüft werden, denn ist eine Wiederherstellung der Daten aus dem Backup nicht möglich, sind diese trotz Sicherungen verloren. Es wird daher empfohlen in regelmäßigen Abständen Wiederherstellungstests der gesicherten Daten durchzuführen. Zur Überprüfung der Wiederherstellbarkeit gehört auch die Analyse, ob und wie auf die Sicherungen zugegriffen werden kann, wenn die Echtdaten im Unternehmen nicht mehr verwendbar sind. Werden die Zugangsdaten und Anleitungen für die Wiederherstellung der Backups zusätzlich an einem weiteren Ort (z.B.: Bank-Safe) aufbewahrt und wissen die entsprechenden Personen über die Aufbewahrungsorte Bescheid.

Zu beachten ist außerdem die Häufigkeit der Sicherungsvorgänge sowie der Speicherort des Backups. Die Häufigkeit kann je nach Provider in der Regel selbstständig konfiguriert werden und es muss abgeschätzt werden, welche Daten zwischen zwei Sicherungen verloren gehen könnten und welchen Schaden dies für das Unternehmen darstellt. Hinsichtlich des Speicherorts ist speziell auf rechtliche Regelungen zu achten, falls Backups in einem anderen Land gespeichert werden. Werden Backups im selben Rechenzentrum abgelegt ist zu hinterfragen, was bei Zerstörung des gesamten Rechenzentrums, zum Beispiel durch Überflutung, geschieht. Hier ist im Wesentlichen zu klären, welche Daten das Unternehmen vor welchen Bedrohungen schützen möchte.

Ebenso zu klären ist, ob die Aufbewahrungsfristen der Backups durch den Cloud-Provider den gesetzlichen Anforderungen an das Unternehmen sowie den unternehmensinternen Bedingungen entsprechen.

Sichere Vernichtung

Für die sichere Vernichtung nach dem Informationssicherheitshandbuch (ISHB) der gespeicherten Daten gibt es wiederum verschiedene Aspekte zu beachten.

Die vollständige und dauerhafte Entfernung von Daten aus der Cloud gestaltet sich nicht immer einfach. Einerseits müssen die Echt-Daten vollständig von den Systemen des Cloud-Providers entfernt werden, aber auch alle Formen von Backup-Daten müssen identifiziert und sicher gelöscht werden. Anbieter von Cloud-Diensten bieten zwar teilweise die Vernichtung der Daten auch innerhalb der Backups an, dies ist aber in der Regel mit starken

Mehrkosten verbunden. An dieser Stelle muss das Risiko abgeschätzt werden, das entsteht wenn die Backups erst im Laufe der Zeit automatisch überschrieben werden.

Die Vernichtung der Daten gestaltet sich daher nicht immer als einfacher und insbesondere nachvollziehbarer Prozess. Aus diesem Grund steht der Cloud-Provider in der Pflicht effektive und vor allem transparente Vorgehensweisen zum sicheren Löschen von Daten anzubieten. Zusätzlich ist es die Aufgabe des Kunden dafür zu sorgen, dass entsprechende Verfahren und Zeitpunkte zum Vernichten von Daten vertraglich geregelt sind.

Verschlüsselung

Der Cloud-Provider ist in der Pflicht die verwendeten Verschlüsselungsverfahren und –Methoden transparent darzustellen, sowie nach dem Stand der Technik sichere Verfahren anzubieten. Im Zuge dessen sollte der Cloud-Provider veraltete und unsichere Kommunikations- und Verschlüsselungsverfahren nicht zur Verfügung stellen bzw. keine Verbindung über diese Kanäle zulassen.

Verwendet der Cloud-Provider proprietäre und/oder unveröffentlichte Verschlüsselungsverfahren ist die Verwendung dieses Anbieters zu hinterfragen, da diese Protokolle erfahrungsgemäß fehleranfällig sind.

Eine Möglichkeit zur Verschlüsselung, die von Cloud-Providern angewendet wird, ist Information-Rights-Management. Bei dieser Methode werden die Daten verschlüsselt und können anschließend nur noch von jenen gelesen werden, die einen korrekten Schlüssel besitzen.

In punkto Verschlüsselung gibt es grundsätzlich zwei verschiedene Punkte die zu betrachten sind. Im Wesentlichen wird zwischen Transportsicherheit und Verschlüsselung der gespeicherten Daten unterschieden.

Storage

Die Verschlüsselung des Storage betrifft die unmittelbar in der Cloud abgelegten Daten, die Echtdaten sowie die Backup-Sicherungen. Es ist zu beachten, dass verschiedene Cloud-Provider keine Verschlüsselung der abgelegten Daten unterstützen. Für das Unternehmen bedeutet dies, zu bewerten ob die Daten in verschlüsselter Form abgelegt werden sollen oder ob das Risiko, dass diese Daten öffentlich eingesehen werden kann, eingegangen wird. Aber auch bei der Verwendung von internen Verschlüsselungsmethoden der Cloud-Provider ist zu bewerten, ob die Mitarbeiter des Providers Einsicht auf die Daten nehmen können oder

nicht. Zur Steigerung der Sicherheit kann eine neutrale, transparente Sicherheitsschicht zwischen Cloud und lokaler Anwendung etabliert werden. Konkret bedeutet das, dass die Verschlüsselung der Daten bereits lokal am Computer des Benutzers durchgeführt wird und erst anschließend ein Upload in die Cloud erfolgt. Erreicht werden kann dies beispielsweise mit EncFS, TrueCrypt, GnuPrivacyGuard oder bestimmten Content-Delivery-Netzwerken.

Transportsicherheit

Verschlüsselung der Daten während diese übertragen werden wird als Transportsicherheit bezeichnet. Dies betrifft im Cloud-Umfeld alle Daten, die vom Client in die Cloud oder umgekehrt, aber auch alle Datenübertragungen zwischen den einzelnen Cloud-Services wie der Applikation und der Datenbank, übertragen werden. Während jedem Datenaustausch ist sicherzustellen, dass die Daten auf einem sicheren Kommunikationskanal übertragen werden.

Die Prüfung dieser Sicherheit betrifft alle verwendeten Kommunikationskanäle und –Protokolle, wie beispielsweise FTP, HTTP, SSH, RemoteDesktop, usw.

Auswahl des Rechenzentrums

Lage

Die Frage, in welchem Land der Cloud-Provider agiert bzw. in welchem Land die Daten abgelegt werden, ist in Abhängigkeit der zu speichernden Daten zu treffen. Speziell ist darauf zu achten, dass nicht nur die Daten aus dem geschäftlichen Alltag betroffen sind, sondern auch gesicherte Backups. Im Konkreten ist hier auf rechtliche und innerorganisatorische Richtlinien und Vorschriften zu achten.

Verschiedene Anbieter geben bereits an in welchen Ländern die Daten abgelegt werden bzw. die wo physischen Rechenzentren liegen. Bei der Auswahl des Landes sind verschiedene Aspekte zu beachten. Einerseits ist die rechtliche Situation in diesem Land von Bedeutung, also im Speziellen die Verpflichtungen, die die Rechenzentren zu erfüllen haben und wie gesetzliche Regulationen sich auf die Formen Datenspeicherung und Datenübertragung, beispielsweise verschlüsselte Übertragung, auswirken. Auf der anderen Seite ist die allgemeine Situation des Landes zu betrachten. Faktoren in dieser Überlegung sind beispielsweise die Wahrscheinlichkeit von Kriegen oder Naturkatastrophen.

Standards

Verschiedene Cloud-Provider arbeiten mit Rechenzentren die nach Sicherheitsstandards wie ISO/IEC 27001 zertifiziert sind. Dieses Zertifikat garantiert zwar nicht, dass die Daten beim Anbieter vollständig sicher sind, es kann jedoch davon ausgegangen werden, dass der Provider bestimmte Maßnahmen zur sicheren Datenverarbeitung ergriffen hat. Eben diese Forderung wird vom österreichischen Datenschutzgesetz an die Unternehmen gestellt.

Forderung nach Transparenz

Auf den vorangegangenen Seiten wurde mehrfach von Transparenz seitens des Cloud-Anbieters gesprochen. Dies basiert primär auf der Tatsache, dass es zahlreiche Anbieter von Cloud-Diensten gibt, die teilweise proprietäre Software bzw. Mechanismen verwenden. Der Kunde kann sich bei Verwendung solcher Lösungen nur auf die Zusage des Betreibers verlassen, selbst aber keine funktionale Prüfung der tatsächlichen Features durchführen bzw. durchführen lassen.

Werden transparente Verfahren und Methoden verwendet, können diese von unabhängigen Experten auf Sicherheit, Compliance, Performance und Funktionalität geprüft und bewertet werden. In Folge dessen sind Endkunden in der Lage diese Features mit anderen zu vergleichen und können auf die Meinungen mehrere Experten vertrauen anstelle eines einzelnen Anbieters.

Offenlegung

In erster Linie muss der Cloud-Provider seine Vertrags- und Geschäftsbedingungen nachvollziehbar und transparent offenlegen. Dies betrifft im Besonderen die Zugriffe und Konfigurationen die dem Betreiber und eventuellen Dritt-Unternehmen gestattet sind und ob in weiterer Folge Einblick auf die Daten des Kunden erlangt werden kann.

Auch die bereits angesprochenen physischen Orte der Datenspeicherung sind von der Offenlegung betroffen. Der Cloud-Provider sollte seine Kunden von sich aus über die rechtlichen Besonderheiten in jenen Ländern informieren, in denen Daten abgelegt werden.

Ebenso sollte sichergestellt werden, dass der Provider den Kunden ggf. über Subkontraktor-Verhältnisse mit anderen Providern sowie Eigentümerverhältnisse informiert. Dies ist beispielsweise in den EU-Standardvertragsklauseln, welche im Kapitel Compliance näher erläutert werden, inkludiert.

Der Kunde sollte in jedem Fall die Offenlegung aller Verfahren und Methoden in Zusammenhang mit der Verwendung der Cloud-Dienste fordern. Dies betrifft unter anderem die Verwendung von Verschlüsselungsmethoden, Authentifizierungsmechanismen, Sicherungskonzepte und notwendige Client-Software bzw. Plug-Ins.

Auditing

Hat der Cloud-Provider Audits zur Sicherstellung von Verfügbarkeit, Compliance, Sicherheit oder anderen Bereichen durchgeführt, so sollten im Sinne der vollständigen Offenlegung die Ergebnisse dieser Audit-Berichte von Ihnen als Kunden unbedingt gefordert werden.

Wurden bisher keinerlei Audits durchgeführt so ist zu prüfen ob über diesen Anbieter Expertenmeinungen bzw. –Bewertungen existieren. Sind in diesem Zusammenhang keinerlei Informationen vorhanden ist es empfohlen Rücksprache mit dem Anbieter über die Gründe dafür zu halten.

Zusammenfassung

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

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

Im nächsten und letzten Kapitel der Reihe befassen wir uns mit dem Ausstieg aus der Cloud – und möglichen Gründen, aus denen man gar nicht erst in die Cloud geht.

Literaturverzeichnis

Accenture. (2012). *Building your Cloud Strategy with Accenture.*
Accenture. (2012). *Cloud Computing*.
Accenture. (2012). *Cloud Market Insight.*
Arbitter, P., Deutsch, P., Pracht, T., & Retti, M. (2011). Cloud Computing - mehr als nur industrialisierte IT. In C. Köhler-Schulte, *Cloud Computing: Neue Optionen für Unternehmen* (S. 35-48). Berlin: KS-Energy-Verlag.
Beckereit, F. (2011). Quo vadis Virtualisierung - Infrastrukturen für die Private Cloud. In C. Köhler-Schute, *Cloud Computing: Neue Optionen für Unternehmen* (S. 67-89). Berlin: KS-Energy-Verlag.
Brunetti, R. (2011). *Windows Azure Step by Step.* Sebastopol: O'Reilly Media.
BSI. (8. 12 2013). *Bundesamt für Sicherheit in der Informatik*.
Bundesamt für Sicherheit in der Informationstechnik - BSI. (02 2012). *Cloud Computing Eckpunktepapier.* F
Bundeskanzleramt. (2012). *Österreichisches Informationssicherheitshandbuch - Cloud Strategie.* Wien: Bundeskanzleramt.
Bundeskanzleramt Rechtsinformationssystem. (2000). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, Fassung vom 13.12.2013*.
Cordial, A. (2011). *Cloud Computing: Immer in Richtung Cloud*.
Gartner Group. (2012). *Special Report Cloud Computing*.
Giedke, A. (2013). *Cloud Computing: Eine wirtschaftsrechtliche Analyse mit besonderer Berücksichtigung des Urheberrechts.* München: Herbert Utz.
Höllwarth, T. (2011). *Cloud Migration* (1. Auflage 2011 Ausg.). Heidelberg: mitp.
Halpert, B. (2011). *Auditing Cloud Computing - A Security and Privacy Guide.* (J. W. Inc., Hrsg.) CA: Wiley.
Hogan, B. (2011). *HTML5 & CSS3: Webentwicklung mit den Standards von morgen.* Köln: O'Reilly.
Hong, H. L., & Fenn, J. (21. 08 2013). *Gartner.*
IDC. (2008). *IDC eXchange*. A
Krishnan, S. (2010). *Programming Windows Azure: Programming the Microsoft Cloud.* Sebastopol: O'Reilly Media.
Kuppinger, M. B. (19. 09 2012). *Cloud und BYOD fordern das Identity-Management*.
Mörsdorf, D. (14. 07 2011). *GfK Austria.*
Masak, D. (2007). *SOA ? Serviceorientierung in Business und Software.* Wiesbaden, DE: Springer Berlin Heidelberg New York.
Mathew, J., Sarker, S., & Varshney, U. (2004). M-Commerce Services: Promises and Challenges. *Communications of the Association for Information Systems: Vol. 14* .
Meir-Huber, M. (2011). *Cloud Computing - Praxisratgeber und Einstiegsstrategien.* Wien, 2010: entwickler.press.
Metzger, C., Reitz, T., & Villar, J. (2011). *Cloud Computing - Chancen und Risiken aus technischer und unternehmerischer Sicht.* München.
Microsoft. (1. 2 2004). *Microsoft Developer Center*.
Moritz Borgmann, T. H. (2012). *On the Security of Cloud Storage Services.* Darmstadt: Fraunhofer Institue for Secure Information Technology SIT.
NACHWEIS FÜR SICHERE CLOUD: „ISO 27001 WIRD VON KUNDEN AKZEPTIERT UND VERLANGT“. (März 2013).

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

Internet-Links

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