INHALTSVERZEICHNIS

CLOUD ODER DESKTOP COMPUTING

EINE ABWÄGUNG DER ARGUMENTE

Wenn es in Computer-Diskussionsforen, bei Anschaffungsentscheidungen für neue Software oder bei der Systemberatung um das Thema Cloud geht, ist häufig ein überzeugtes „Nein, ich gehe nicht in die Cloud“ zu hören. Solche bisweilen fast sogar stur, bockig vorgetragenen Ankündigungen werden dann beim Nachhaken regelmäßig mit Sicherheitsbedenken, Ängsten vor Ausspähung und Kontrollverlust begründet. Zeit, sich etwas intensiver und vielleicht auch rein sachlich ohne jegliche Emotion mit dem Thema Cloud und der Alternative Desktop-Computing zu beschäftigen. Es soll hier ganz bewusst nicht euphorisch der Cloud das Wort geredet werden.

VORBEMERKUNG

Zuallererst muss man sich wohl klarmachen, dass wir - bei aller Ablehnung der Cloud durch manche Zeitgenossen - doch schon vermutlich alle längst in der Cloud angekommen sind, diese vielfach bereits intensiv nutzen. Angefangen bei den Millionen Nutzern von Smartphones – wer da nicht intensiv an den Grundeinstellungen herumschraubt und viele Möglichkeiten und Dienste gar nicht erst nutzt, wird bereits jetzt regelmäßiger Cloud-Nutzer sein: Das fängt bei der Synchronisierung von Adress- und Kalenderdaten vom heimischen Rechner auf das Smartphone und zurück an, geht über den Abgleich der Browser-Favoriten und die Übertragung aller mit dem Smartphone gemachten Fotos weiter. Wie selbstverständlich nutzen viele zudem Speicherdienste wie Dropbox, Onedrive oder iCloud mit Ihren Mobilgeräten und lassen sich von cloud-basierten Sprach-Assistenten wie Siri und Cortana oder der Google Maps Navigation helfen. Der moderne, mobile Mensch ist ohne die Synchronisations- und Speicherdienste der Cloud und sein Smartphone kaum mehr vorstellbar.

Aber auch in anderen Bereichen der Computer-Nutzung hat die Cloud längst Einzug gehalten. Wer einen Online-Shop betritt, wird von Cookies und Google Analytics registriert, gespeichert und nachverfolgt, selbst wenn er keine Bestellung tätigt. Online-Shopping aber ist für eine zunehmende Zahl von Kunden heute gelebter Alltag und was ist das anderes als die Nutzung der Cloud – Sie hinterlegen in einem Shop Ihre Daten, ihre Einkäufe, Ihre Zahlungsmodalitäten und Lieferwünsche.

Nicht anders ist es bei der Nutzung von modernen Formen der Kommunikation oder des Gedankenaustauschs. Ob nun Skype, What´sApp, Foren aller Art oder Facebook, Xing und LinkedIn. Kaum jemand, der nicht wenigstens einen dieser Cloud-Dienste nutzt und teilweise sehr offenherzig und freiwillig mit allerlei Daten füttert. Vergessen Sie nicht – auch Email ist ein cloud-basierter Dienst, denn hinter jeder Mail steckt ein Mail-Server irgendwo bei Ihrem Mail-Provider.

Und woher kommt es, dass immer mehr Bankfilialen schließen? Weil wir allesamt immer mehr und wohl bald nur noch Online-Banking betreiben und unsere Geldanlage über Direktanlagebanken im Internet tätigen. Gleiches gilt mehr und mehr für die Versicherungsbranche, den Preisvergleich für Gas und Strom und die Buchung der nächsten Urlaubsreise.

Fazit: In der Regel wird es also gar nicht um die grundsätzliche Entscheidung „Cloud nutzen oder nicht“ gehen, sondern höchstens um die Frage „Wieviel Cloud wofür?“ gehen können.

SICHERHEITSBEDENKEN

Bei der Cloud-Kritik steht ein Punkt immer wieder an vorderster Stelle – die Sicherheit. Und sich um die Sicherheit zu sorgen, ist auch allzu verständlich, vor allem dann, wenn man an Hacker-Attacken, Leaks, Indiskretionen und Datenklau denkt. Kaum ein Großunternehmen oder Webportal, das nicht schon mal

angegriffen und häufig auch erfolgreich ge-hacked worden ist. Daher geben viele ihre Daten nur ungern aus der Hand, stehen einer Speicherung in der Cloud und damit bei Dritten äußerst skeptisch gegenüber.

Es stellt sich aber in einer technisch komplizierten Zeit die Frage, ob wir selbst auf unseren eigenen Systemen denn für mehr Sicherheit unserer Daten sorgen können. Irgendwo müssen die Daten ja schließlich gespeichert werden. Die Zeiten, in denen noch alles auf Papier erstellt und dann eben auch auf Papier archiviert wurde, sind ja inzwischen für viele vorbei. Bei digitalen Inhalten wie Websites, Videos, CAD-Zeichnungen, Kalkulationstabellen uvm. kommt gar keine andere Speicherform als die digitale in Betracht.

Niemand kann es mit letzter Sicherheit sagen, aber es gibt Zahlen über gekaperte Rechner, infizierte Systeme und sogenannte Bot-Netze (Rechner, die von Hackern ferngesteuert werden können), die von Millionen unsicherer Systeme ausgehen. Schon 2015 schrieb der Spiegel von bis 40% infizierten Rechnern in Deutschland. Das sollte zu denken geben, Ihre Systeme könnten dazugehören.

Selbstverständlich wird ein sicherheitsbewußter Anwender ein Antivirus-Programm einsetzen, keine Mail-Anhänge aus verdächtigen Quellen öffnen und auf keine Phishing-Mail hereinfallen. Beherrschen wir alle aber unsere Systeme so sehr, dass uns nie etwas Derartiges passieren kann? Und wenn es passiert ist, würden wir es merken? Schließlich wird der Hacker nicht vor der Tür stehen, klingeln und uns ein Präsent-Paket mit der Aufschritt „Sie sind ge-hacked worden“ überbringen, sondern klammheimlich seinen Zugriff auf unser System nutzen. Und wenn er das tut, wäre jeder von uns in der Lage, dem einen Riegel vorzuschieben, die Sache zu beenden?

Wenn es um Wartung, Pflege und Reparatur eines Autos geht, ist für die meisten selbstverständlich, das Auto in eine Fachwerkstatt zu bringen, zu Leuten, die das gelernt haben. Dabei haben wir sogar einen Führerschein. Den Computer bedienen wir häufig ohne jegliche fachliche Ausbildung und Expertise, aber die Sicherheit haben wir besser im Griff als die Netzwerk-Administratoren, Systemanalytiker und Informatiker in einem Rechenzentrum? Ernsthaft?

Umgekehrt muss man eigentlich denken. Die erfolgreichen Angriffe durch Hacker auf Rechenzentren zeigen, dass es selbst Vollprofis schwerfällt, einen 100prozentige Sicherheit herzustellen. Wie aber wollen wir Laien das dann erreichen? Am ehesten noch dadurch, dass wir uns entweder ganz vom Netz abkoppeln (was wohl kaum geht) oder daraufsetzen, dass die von uns gespeicherten Inhalte ausnahmslos niemanden interessieren.

Und auch bei anderen Sicherheitsaspekten dürfte jedes Rechenzentrum mehr leisten, als wir es privat oder in unserer kleinen bis mittelständischen Firma je darstellen können.

Wie sieht es etwa mit der Sicherung von Daten, der Erstellung von Backups aus? Werden bei uns Daten automatisch gespiegelt, regelmäßig zusätzlich gesichert, auf andere Systeme ausgelagert und an weiteren Standorten noch mal gespeichert? Bei professionellen Rechenzentren ist das im Rahmen von Zertifizierungen Standard. Fragen Sie sich mal, wie oft Sie selbst schon Daten verloren haben und wie oft es passiert ist, dass die HTML Seiten Ihrer Website beim Hosting-Provider einfach „weg“ waren? Wir von INtex betreiben seit 1999 eine Website und in dieser Zeit ist noch keine einzige Seite auf den Servern unserer Provider je „verschwunden“.

Was ist in unseren Büros getan worden, um Rechner, Festplatten und Sicherungssysteme vor den Folgen höherer Gewalt wie Feuer, Sturm, Flut und Erdbeben zu schützen? Gibt es eine Sprinkleranlage, einen Überflutungsschutz, sichere Montage der Rechner-Systeme, redundante Stromversorgung? Rechenzentren haben so etwas.

Und schließlich der Zugriff durch Dritte – gibt es bei uns eine Zugangskontrolle, einen Sicherheitszaun, Alarmanlagen, Kameras und anderen Einbruchschutz, um den Zugriff auf unsere Gebäude, Büros und Computer-Systeme zu beschränken? Auch das gibt es bei Rechenzentren.

Es bleibt somit eigentlich nur ein Punkt, der in einem Rechenzentrum leichter passieren kann, als bei Ihnen im Hause – jemand von den im Rechenzentrum beschäftigen Administratoren schaut auf Ihre Daten, bedient sich gar daran in eigenem Interesse.

Zunächst aber gibt es die juristisch einklagbare Vereinbarung zur Auftragsdatenvereinbarung (bei INtex hier …), die den Mitarbeitern des Rechenzentrums eine „Selbstbedienung“ an ihren Daten untersagt und diese sowie deren Arbeitgeber dafür haftbar macht. Mit dieser Vereinbarung und einem Server-Standort in Deutschland sind übrigens auch Sie als Auftraggeber auf der rechtlichen Seite abgesichert.

Wenn es aber zu Zugriffen kommt, wird es wohl in der Regel in Ihrem Auftrag, nämlich zu Support-Zwecken sein. Und darin unterscheidet sich die Cloud dann wieder nicht mehr sehr vom Desktop-Computing. Natürlich kann der Support in vielen Fällen nur helfen, indem er sich mit Ihren Eingaben in die Systeme vertraut macht, denn viele Fehlfunktionen rühren von Fehleingaben her. Beim Cloud-Computing hat der Support dazu direkten Zugriff auf die Daten, beim Desktop Computer in Ihren Räumen würde er sich mit einer Software wie TeamViewer auf Ihr System einklinken. Und dann sieht der Supporter ebenfalls Ihre Daten oder zumindest Teile davon – aber wie soll es auch anders gehen? Wenn das Auto repariert werden muss, fahren Sie es ja auch in die Werkstatt und überlassen es den Fachleuten.

Nehmen wir den Paketboten als Analogie. Natürlich schreibt uns der Datenschutz die möglichst sparsame Speicherung von personenbezogenen Daten vor, sieht vielfach eine Anonymisierung und eine strikte Beschränkung des Zugriffs vor, verbietet die Datenübermittlung an Dritte. Dennoch muss der Paketbote eine Kundenadresse erfahren, wenn er ein Paket zustellen soll.

Bleibt also das Restrisiko eines kriminellen Mitarbeiters im Rechenzentrum. Dieser könnte – aus welchen Gründen auch immer – an Ihren Daten interessiert sein und damit Missbrauch betreiben. Ob dieses Risiko höher ist, als dass ein Mitarbeiter aus Ihrem eigenen Hause gleiches tut, Computer bei Ihnen gestohlen oder Ihre Rechner von außen angegriffen werden, müssen Sie selbst entscheiden.

Vielfach wird hier auch die platte Weisheit greifen – „Wer nichts zu verbergen hat, braucht auch nichts zu befürchten.“ Und immer gilt: 100prozentige Sicherheit gibt es nicht. Weder im Rechenzentrum, noch auf Ihren Systemen.

Nach meinem Dafürhalten kann man als vorsichtiges Fazit aus diesen Überlegungen festhalten, dass die Cloud bzw. die Rechenzentren zumindest nicht eklatant mehr und größere Risiken aufweisen als das Desktop Computing. Stellt sich also die Frage, ob die Cloud denn eventuell Vorteile gegenüber dem Desktop aufweist, die auch die letzten Sicherheitsbedenken überwinden können, als das geringere Übel erscheinen lassen?

VORTEILE DER CLOUD

Die technischen Vorteile der Cloud kann man kurz so zusammenfassen:

- Standort-Unabhängigkeit: Da Sie über das Internet auf Anwendungen und Daten zugreifen und das Netz mehr oder minder überall und immer zur Verfügung steht, können Sie jederzeit und überall Programme und Daten aus der Cloud nutzen. Wenn bei den Daten auf zentrale Speicherung (Client Server) statt auf Synch gesetzt wird, sind diese Daten zudem immer sicher aktuell.
  Natürlich können Sie auch Daten und Programme auf einem Laptop mitnehmen, diese sind aber mitunter nicht aktuell, einer gewissen Verlustgefahr ausgesetzt (Laptop-Klau) und vielleicht auch nicht komplett (Speicherkapazität des Rechners reicht im Zweifel nicht für alle Firmendaten).
  Alternativ könnten Sie noch einen eigenen Server über das Internet zugänglich machen. Ob das allerdings viel sicherer als die Nutzung eines Rechenzentrums ist, kann man bezweifeln. Außerdem müsste Ihr Server schon so gut an das Internet angebunden sein, wie ein Rechenzentrum, um für die Anwender die gleiche Geschwindigkeit beim Daten- und Programmzugriff zu gewährleisten. Das ist in

der Regel aber nicht der Fall.
Die Cloud ist natürlich keine Lösung in Regionen, in denen kein oder kein schnelles Internet zur Verfügung steht. Aufgrund der Bedeutung des Netzes für die Infrastruktur kann man aber wohl davon ausgehen, dass diese Situation von Jahr zu Jahr besser wird.

- System-Unabhängigkeit: Cloud-Anwendungen laufen entweder als WebApp im Browser und damit auf jedem Betriebssystem oder es stehen vielfach für gängige Cloud-Dienste auch Apps für alle weiter verbreiteten Betriebssysteme zur Verfügung. Die meiste Desktop-Software dagegen ist etwa mobil mit einem Smartphone nicht zu gebrauchen.
- Geräte-Unabhängigkeit: Über die System-Unabhängigkeit hinaus sind Cloud-Anwendungen – hier vor allem auch wieder die WebApps – völlig unabhängig vom genutzten Gerät. Responsive Oberflächen nutzen vom kleinsten Smartphone Display bis hin zum größten Präsentations-Display alle Bildschirmgrößen, lassen sich mit der Maus, Tastatur oder Finger bedienen. Eine Standardoberfläche steht immer und überall zur Verfügung, die Software ist also jederzeit nutzbar und leichter erlernbar als x Varianten mit unterschiedlichen Funktionsumfängen.
  Ganz nebenher erleichtert dies auch die Einrichtung der in der Firma benutzten Geräte. Da ja nichts für die Cloud-Lösung extra installiert werden muss, keine Daten zu kopieren sind, geht die Einrichtung schnell – sowohl bei neuen Geräten, also auch bei Austausch-/Leihgeräten und Reparatur-Rückläufern. Der Mitarbeiter ist in allen Fällen im Nu arbeitsfähig.
- Zukunftssicherheit: Aus der System- und Geräteunabhängigkeit ergibt sich bei der Cloud auch eine erhebliche Zukunftssicherheit für Ihre Investition. Ob Apple etwa wieder auf ARM Prozessoren umsteigt, nur noch 64 Bit Software zulässt, iOS und MacOS Apps auf eine gemeinsame Plattform hievt oder etwa der MacApp Store zur einzigen Quelle von Software wird, kann Ihnen mit einer Cloud-Lösung herzlich egal sein. Einen funktionierenden Browser für das Betriebssystem wird es immer geben. Ebenso verhält es sich mit den Geräten und Geräte-Typen – ob Microsoft nun ein Surface Phone jemals vorstellt, Apple den Mac mini abschafft – all das braucht Sie mit einer Cloud-Lösung nicht zu kümmern. Es wird immer andere Geräte geben, die mit einem Browser auf die Cloud zugreifen können.
- Mobilität: Aus Standort-, System- und Geräte-Unabhängigkeit erwächst eine früher unbekannte Mobilität. Der Arbeitsplatz kann zu jeder Zeit überall sein. Man braucht im Zweifel nicht mal ein eigenes Gerät, ein Computer etwa in der Hotel-Lobby tut es auch.
- Team-Fähigkeit: Im Übrigen sind Cloud-Dienste und Anwendungen immer und von vornherein auch Netzwerkdienste und somit teamfähig. Desktop-Software dagegen ist häufig reine Einzelbenutzer-Software. Team-Fähigkeit kann sogar für Einzelkämpfer interessant sein, wenn es um die Zusammenarbeit mit Kunden und Interessenten geht – diese lassen sich bei einer Cloud-Lösung ganz anders einbinden.

Fazit: Die Cloud bietet für mobile, vernetzt-arbeitende Teams an unterschiedlichen Standorten, die verschiedenste Geräte und Betriebssysteme nutzen, erhebliche Vorteile gegenüber einer Desktop-Software-basierten IT-Infrastruktur. Die Vorteile nehmen natürlich mit Wegfall einzelner Merkmale ab. So hat ein Einzelkämpfer/Selbständiger weniger von der Team-Fähigkeit als eine Projektgruppe, jemand der ausschließlich in seinem Büro sitzt, wenig von der Mobilität und wer nur einen Computer nutzt und weder Tablet noch Smartphone hat, kaum etwas von der Geräte- und Systemunabhängigkeit, es sei denn sein Computer geht kaputt oder kommt in die Jahre und muss ausgetauscht werden. Hier wird also jeder für sich die Sachlage prüfen müssen.

Wenn es um die Nutzung von Software in Teams geht, bietet die Cloud auch noch Preisvorteile, sofern die Cloud-Dienste gemietet werden. Dann nämlich kann über flexible Mietverträge nur die IT-Infrastruktur gebucht werden, die ein Unternehmen zum jeweiligen Zeitpunkt auch wirklich benötigt. Wer etwa ein starkes Weihnachtsgeschäft hat, aber einen schwachen Sommer, der kann im Winter Arbeitsplatzlizenzen und Server-Kapazitäten hinzubuchen und zum Sommer hin wieder abbestellen. Die IT kostet und leistet dann jeweils nur so

viel wie auch benötigt wird. Ebenso kann die Cloud viel flexibler als eine eigene IT Infrastruktur schnell wachsende Anwenderzahlen bedienen.

Gekaufte Desktop Computer, Server und Software dagegen reißen bei der Investition ein großes Loch in Ihr Budget und werden hinterher möglicherweise gar nicht in der Intensität benötigt wie ursprünglich gedacht – das wäre dann eine klassische Fehlinvestition, die Sie mit der Cloud vermeiden können.