

# Sicherer Datenaustausch in der Cloud

**Virtuelle Teams, externe Partner: Die standortübergreifende Zusammenarbeit wird immer wichtiger und erfordert Lösungen für den Austausch umfangreicher Daten und Dokumente. Diese bereitzustellen, ist für viele IT-Organisationen eine echte Herausforderung – insbesondere, wenn es dabei um sensible Informationen und die Einhaltung von Datenschutzvorgaben geht. Mangels praktikabler Alternativen greifen viele Firmen auf E-Mail beziehungsweise File Transfer (FTP) zurück. Dabei sind E-Mails nicht mehr als ein Workaround, der nie für den Datenaustausch gedacht war, während FTP-Lösungen häufig großen administrativen Aufwand nach sich ziehen und umständlich zu bedienen sind. Die Cloud hingegen bietet viele neue Möglichkeiten, die sie zur idealen Sharing-Plattform machen. So haben Dienste wie Dropbox und Co. unter Privatanwendern bereits weite Verbreitung gefunden – Firmen fürchten jedoch meist den Kontrollverlust. Daher sind beim Einsatz im Unternehmen Services gefragt, welche die Vorteile der Cloud mit ergänzenden Sicherheitsmaßnahmen und einem durchdachten Implementierungskonzept verbinden.**

Für den Austausch von Unternehmensdaten bietet sich die Cloud als interessante Alternative zu den üblichen Lösungen an. Sie stellt praktisch unbegrenzten Speicherplatz bereit, der sich flexibel an den aktuellen Bedarf des Unternehmens anpasst und kostengünstig verfügbar ist. Während sich viele andere Lösungen als aufwändig und supportintensiv erweisen, bietet die Cloud die Möglichkeit, administrative Aufgaben zu günstigen Konditionen auszulagern und so den Inhouse-Aufwand zu reduzieren.

Aufgrund der Flexibilität der Cloud sind viele Einsatzszenarien denkbar: So bietet

sich einerseits die Nutzung für den Datenaustausch zwischen verschiedenen Standorten eines Unternehmens an. Hier stellt eine Cloud-basierte Lösung eine attraktive Alternative zur relativ aufwändigen Anbindung per Virtual Private Network (VPN) dar. Doch auch für die Zusammenarbeit über Firmengrenzen hinaus ist die Cloud geeignet. Als Collaboration-Plattform ermöglicht sie auch den einfachen Zugriff von externen Partnern, Kunden oder Zulieferern. Daneben lässt sich über die Cloud auch der automatische Datenaustausch per Electronic Data Interchange (EDI) und damit die Kommunikation zwischen Anwendungs-

systemen verschiedener Organisationen realisieren.

## Cloud & Security: Sicherheit auf mehreren Ebenen

Dank der vielen Vorteile und möglichen Einsatzszenarien spricht also vieles für die Cloud als Plattform für den Austausch von Dokumenten und Daten. Trotzdem halten viele Unternehmen weiterhin an Technologien wie E-Mail und FTP fest. Der zentrale Grund sind Sicherheitsbedenken: Was passiert mit meinen Daten in der Cloud? Inwiefern kann ich selbst darauf Einfluss nehmen? Aus Angst vor dem Kontrollverlust scheuen viele Firmen den Schritt in die Cloud. Anstatt sich jedoch in der Konsequenz mit den Unzulänglichkeiten der scheinbar alternativlosen Workarounds zu arrangieren, sollte man die Gelegenheit nutzen und sich von althergebrachten Vorstellungen von IT-Security verabschieden. Sicherheit in der Cloud begreift sich als Zusammenspiel mehrerer Ebenen. Konkret bedeutet das, die Mechanismen der Cloud zu nutzen, diese jedoch durch zielgerichtete Maßnahmen zu ergänzen.

In vielerlei Hinsicht bietet die Cloud tatsächlich mehr Sicherheit als das eigene Rechenzentrum: Homogene Infrastrukturen und die Automatisierung vieler Prozesse



ermöglichen es den Cloud-Anbietern, viele sicherheitsrelevante Aufgaben deutlich effizienter durchzuführen, als dies in firmeneigenen, meist historisch gewachsenen Umgebungen möglich ist. Hier lohnt es sich durchaus, Verantwortung abzugeben.

Wenn es aber um die Vertraulichkeit und Integrität kritischer Daten und die Einhaltung von Datenschutzvorgaben geht, reichen die genannten Mechanismen freilich nicht mehr aus. Daher sind intelligente Cloud Services gefragt, die auch höchstem Schutzbedarf gerecht werden: mit zusätzlichen Sicherheitsmaßnahmen, die dem Eigentümer der Daten die volle Kontrolle über seine Informationen gewährleisten – nicht zuletzt, weil dieser im Falle einer etwaigen Datenschutzverletzung auch die volle Verantwortung trägt. Doch welche Voraussetzungen muss ein solcher Service erfüllen?

### Die Kontrolle liegt beim Dateneigentümer

Ein wichtiger Aspekt ist zunächst einmal der physische Standort der Cloud-Rechner. Darauf sollte der Kunde Einfluss nehmen können, denn in vielen Fällen gelten hier strikte Datenschutzvorgaben wie etwa die des Bundesdatenschutzgesetzes (BDSG). So sind beispielsweise deutsche Rechtsanwaltskanzleien dazu verpflichtet, sensible Daten ausschließlich auf Servern in Deutschland abzulegen. Eine sinnvolle Lösung muss solche Einschränkungen berücksichtigen.

Auch eine Logging-Funktion, im Zusammenspiel mit einer effektiven Zugriffskontrolle, ist Voraussetzung: Nur wenn alle Vorgänge detailliert und auf Dateiebene protokolliert werden, lässt sich der Zugriff auf die Daten vollständig nachvollziehen und etwaiger Rechtemissbrauch aufdecken.

Die zentrale Voraussetzung für eine einsatzfähige, Cloud-basierte Sharing-Plattform ist jedoch die Verschlüsselung. Nur so können Vertraulichkeit und Integrität sensibler Daten auch auf fremden Rechnern gewährleistet werden. Hervorzuheben ist hier der Zeit-

punkt der Verschlüsselung: Wichtig ist, dass die Daten bereits verschlüsselt sind, wenn sie das Unternehmensnetzwerk verlassen. Der Encryption Key darf jedoch nicht zusammen mit den Daten in die Cloud gegeben werden, sondern muss zu jedem Zeitpunkt der vollen Kontrolle des Dateneigentümers unterliegen.

Generell sind hier verschiedene Bereitstellungsszenarien denkbar, die sich allerdings in ihrer Komplexität unterscheiden. Die entscheidende Frage lautet also: Welche Lösung ist für den täglichen Einsatz praktikabel, sowohl für den Administrator als auch für den Endanwender?

### Zentrale Verschlüsselung erleichtert Kontrolle

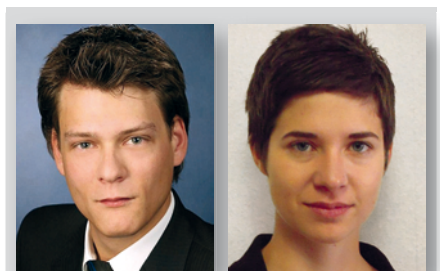
Für eine möglichst einfache Umsetzung empfehlen sich Lösungen, bei denen die Verschlüsselung an zentraler Stelle erfolgt. Dies hat gegenüber einer Verschlüsselungslösung, die auf jedem Client implementiert wird, eine Reihe von Vorteilen: Die Installation entsprechender Software auf allen beteiligten Rechnern entfällt ebenso wie die aufwändige Verwaltung vieler Schlüssel. Werden keine Encryption Keys auf den Clients hinterlegt, so hat auch kein Endanwender die Möglichkeit, auf diese direkt zuzugreifen und sie beispielsweise an unautorisierte Dritte weiterzugeben. Und auch für die Protokollierung hat eine zentrale Verschlüsselung einen bedeutenden Vorteil: Nur so lassen sich Logs mit Informationen über Dateizugriffe zentral sammeln und auswerten. Liegen die Log-Daten dagegen verteilt auf den einzelnen Clients vor, ist eine sinnvolle Analyse und Nutzung der Zugriffsinformationen kaum möglich.

Doch nicht nur die Administration wird vereinfacht, auch die Nutzung durch den Endanwender – denn „zentral“ bedeutet auch immer „transparent“. Das heißt, der Benutzer greift wie gewohnt auf die Dateien in der Cloud zu – Ver- und Entschlüsselung laufen ohne sein Zutun im Hintergrund ab. Dies sorgt für eine einfache Handhabung und einem dementsprechend geringeren Aufwand für Schulungen und Support.

Zur möglichst einfachen Nutzung gehört auch die Bereitstellung intuitiver Benutzerschnittstellen. Der Zugriff sollte über Wege erfolgen, die der Anwender bereits aus seiner täglichen Arbeit kennt. Für interne Anwender bietet sich die Anbindung über Netzwerkfreigaben an, während sich für den Zugriff externer Benutzer Web-Portale eignen. Darüber hinaus sollte die Lösung jedoch viele weitere Schnittstellen unterstützen, damit die Kunden die verschiedenen Interfaces ihrer externen Kommunikationspartner flexibel bedienen können.

Nicht zuletzt ist auch die Integration in die bestehende Umgebung ein entscheidendes Kriterium. Eine Anbindung an interne Verzeichnisdienste wie das Active Directory ist in vielen Unternehmen ein absolutes Muss, damit die bestehende Rechtestruktur auch für den Zugriff auf den Cloud-Speicher genutzt werden kann. Eine praktikable Umsetzung sollte möglichst geringe Anpassungen der bestehenden Infrastruktur erfordern. Lösungen, die hingegen umfangreiche Änderungen voraussetzen, erweisen sich häufig als fehleranfällig, support- und kostenintensiv – und würden so einige der Eigenschaften außer Kraft setzen, die Speicherplatz in der Cloud als Sharing-Plattform gerade so attraktiv machen.

Damit die Cloud also ihre Vorzüge ausspielen kann, ist eine Reihe von Voraussetzungen zu erfüllen. Überzeugende Services müssen es schaffen, die Vorteile von Cloud-Storage mit Sicherheit, Benutzerfreundlichkeit und einfacher Administration zu vereinen – und damit letztlich auch einen Kostenvorteil gegenüber bisherigen Technologien bieten. Dann besitzen sie auch definitiv das Potenzial, bisherigen Workarounds wie E-Mail und FTP den Rang abzulaufen. ■



Björn Matthiessen und Brigitta Strigl,  
secureMSP



Für Abonnenten ist dieser Artikel auch digital auf [www.datakontext.com](http://www.datakontext.com) verfügbar



Weitere Artikel/News zum Schwerpunkt unter [www.datakontext.com/mss](http://www.datakontext.com/mss)