



# Mail & Collaboration in der Cloud

Das derzeitige IT-Modell wurde vor Jahrzehnten für eine Welt entworfen, in der der Nutzer an einem einzelnen Computer, in ein und demselben Büro, in einem gesicherten Netzwerk und hinter der Firewall des Unternehmens arbeitete. Dass sich aber die moderne Kommunikation seit Jahren in einem rasanten Wandel befindet, ist keine Neuigkeit: Smartphones, Notebooks und Tablet-PCs haben sich sowohl im privaten Umfeld als auch in den meisten Unternehmen längst etabliert. Zusätzlich erweitern Chat, IP-Telefonie und Web-basierte Video-Konferenzen die Möglichkeiten der effizienten Kommunikation. Parallel wachsen die technischen Herausforderungen beim Betrieb einer Mail-Infrastruktur ebenso rasant, wie die Datenvolumen der Dateianhänge. Einerseits steigt die Komplexität von Mail & Collaboration-Anwendungen andererseits sind die Anforderungen an solche Lösungen bei den meisten Unternehmen identisch und leisten in der Regel keinen Beitrag zur unternehmerischen Kernwertschöpfung. Die bedarfsgerechte Nutzung eines Mail & Collaboration-Dienstes in Form von Software-as-a-Service (SaaS) kann für Unternehmen eine wirtschaftliche Alternative darstellen. Dabei sind es betriebswirtschaftliche, technische und sicherheitsspezifische Aspekte, die bei der Entscheidung zu beachten sind.

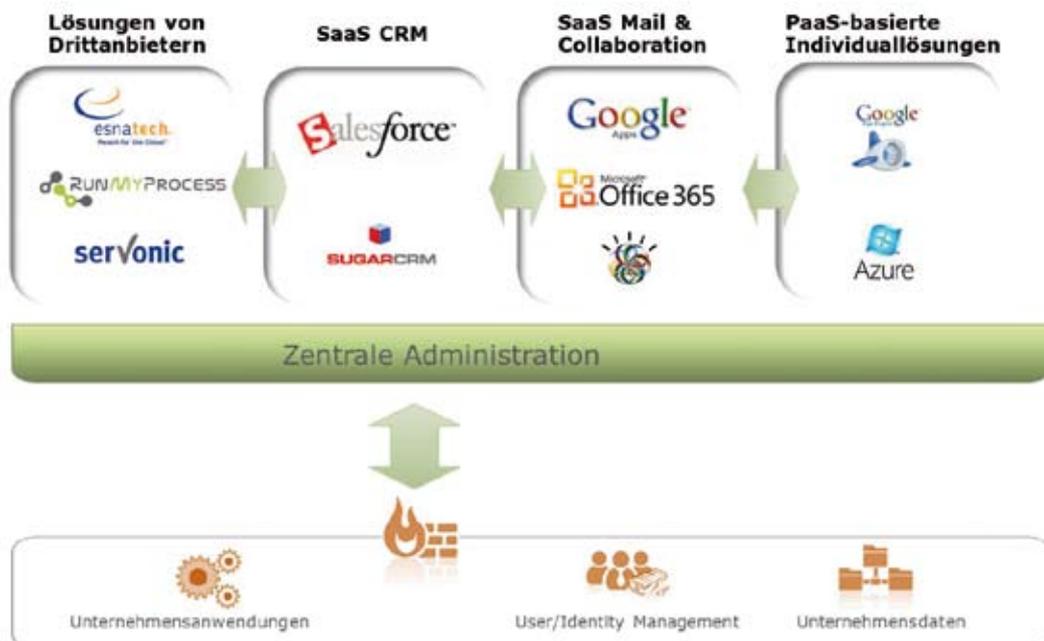
## IT im Wandel

Wie die Unternehmen selbst, ist auch die IT-Infrastruktur ständigen Veränderungen unterworfen. Dabei werden immen-

se Summen in den reinen Erhalt einer IT-Infrastruktur investiert, die den Anforderungen an die moderne Unternehmenskommunikation nur noch zum Teil gerecht wird. Gemäß der Capgemini-Studie „IT-Trends 2012“ werden für die Entwicklung von Innovationen in D-A-CH im Durchschnitt nur knapp 22% des IT-Budgets aufgewendet, von denen zirka ein Drittel in die Evaluierung neuer Technologien und knapp zwei Drittel in Umsetzungsprojekte inklusive Beschaffung, Entwicklung und Implementierung gesteckt werden. Der größte Anteil des Budgets fließt in die Erhaltung der IT-Landschaft: 71% werden für die Aktualisierung von Infrastruktur-Komponenten sowie kleinere und größere Updates und Harmonisierungen ausgegeben. IT-Administratoren müssen dem endlosen Zyklus aus Patches, Upgrades und der Verwaltung der bestehenden Servern und Desktops entkommen.

Aber eine neue Generation von Mitarbeitern erobert die Unternehmen und verlangt vor allem eines: Flexibilität. Die Leistungsfähigkeit von Mitarbeitern wird nicht mehr an den Stunden der Anwesenheit im Büro gemessen, sondern an deren Ergebnissen. Home-Office war gestern. Morgen wird der Zugriff auf wichtige Arbeitsunterlagen und Unternehmensdaten von überall mobil erfolgen. Schon heutzutage arbeitet der Großteil der Arbeitnehmer weltweit zumindest zeitweise außerhalb des Büros. Gemäß den Marktbeobachtern von IDC werden weltweit 35 % der arbeitenden Bevölkerung bis zum Jahr 2013 mobil arbei-

ten, die sich dabei einer sehr heterogenen Endgerätelandschaft bedienen werden. Kein Wunder: Mit dem mobilen Arbeiten zu jeder Zeit und von überall kann ein gewaltiges Plus an Produktivität verbunden sein. IDC geht davon aus, dass schon in diesem Jahr rund 20% aller deutschen Arbeitnehmer mobil arbeiten. In der Bereitstellung dieser Informationen liegt der Schlüssel zu einem zufriedenen Anwender. Und wenn die IT-Abteilung der Nachfrage nicht gerecht wird, nutzen die Anwender Technologien und mobile Endgeräte zur Erreichung ihrer beruflichen Ziele, die sie auch im privaten Umfeld verwenden. „Bring your own Device“ oder kurz „BYOD“ ist ein globaler Trend, der die IT-Verantwortlichen in Deutschlands Unternehmen jedoch noch spaltet: Die einen sehen einen Mehrwert in der verbesserten Wettbewerbsfähigkeit durch die gesteigerte Mobilität. Die anderen hingegen befürchten den Kontrollverlust und IT-Gau durch virenverseuchte und mit Sicherheitslücken versehene Endgeräte. Mit Recht: denn anders als PCs oder Laptops stehen insbesondere die mobilen Endgeräte, die derzeit boomen, nur unter der Administration des jeweiligen Nutzers. Bei Verlust oder Diebstahl sind Kosten für das Ersatzgerät verschwindend gering gegenüber den Folgekosten durch die Störungen im Betriebsablauf oder durch den Datenverlust. 89% der im Juli 2010 von IDC befragten Unternehmen in Deutschland zwischen 50 und 500 Mitarbeiter haben in ihrem Unternehmen den Diebstahl oder Verlust von Laptops erlitten.



---

### Veränderungen sind ein Muss

Cloud-basierte Mail & Collaboration oder CRM-Lösungen bieten den Eintritt in die mobile und browser-basierte Welt. Es wird immer wichtiger, dass Mitarbeiter sowohl innerhalb eines Unternehmens als auch unternehmensübergreifend in Echtzeit zusammenarbeiten können. Beim Cloud Service Provider (CSP) werden sowohl Anwendungen als auch die Daten zentral gespeichert und in einer hochskalierbaren, sicheren und zuverlässigen Multi-Tenant-Infrastruktur bereitgestellt. Viele Anbieter haben inzwischen den Begriff „Cloud Computing“ für sich vereinnahmt. Folgende Vorgehensweisen haben mit echtem Cloud Computing nichts zu tun: z.B. das Hosting von Single-Tenant-Serverlösungen im Rechenzentrum eines Anbieters oder die Virtualisierung vorhandener Infrastruktur und Anwendungen innerhalb des Rechenzentrums eines Kunden

### Sicherheit in der Cloud

Die großen CSPs verfügen über eine komplexe Sicherheitsstrategie, die im Hinblick auf Datenspeicherung, Zugriff und Datentransfer Kontrollmöglichkeiten auf mehreren Ebenen bietet:

- Organisation der Sicherheitsmaßnahmen
- Datenklassifizierung und -kontrolle
- Standort- und Betriebssicherheit
- Systementwicklung und -wartung
- Wiederherstellung im Notfall
- Einhaltung der gesetzlichen Vorschriften.

Die Systeme unterliegen einem konstanten internen und externen Monitoring: 7 Tage die Woche und 24 Stunden am Tag. Die Gründe für die Notwendigkeit der permanenten Überwachung findet man u.a. im Bericht „Die Lage der IT-Sicherheit in Deutschland 2011“, der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Mai 2011 veröffentlicht wurde. Ein Botnetz mit 10.000 Bot-PCs lässt sich beispielsweise für rund 200 US-Dollar pro Tag mieten, so das BSI. Da Botnetze auch aus mehreren Millionen PCs bestehen können, lässt sich das monetäre Potenzial hinter solchen Internetangriffen nur erahnen. Zentrale Dienste in der Cloud sind auf Grund von Skalierungseffekten effizienter als der dezentrale Inhouse-Betrieb komplexer EDV-Strukturen. Zumal der Betrieb von Software nicht nur die Installation, sondern auch unliebsame Aufgaben wie Update-Management, Datensicherung, Gewährleistung der Ausfallsicherheit, Software-Verteilung, Überwachung usw. nach sich zieht.

### Zusammenarbeit endet nicht an der Firewall

Geschäftserfolg war immer schon von effizienter Zusammenarbeit abhängig, aber die Art der Zusammenarbeit hat sich verändert. Unternehmen sind in ein Netzwerk mit Geschäftspartnern, Lieferanten und Kunden eingebunden. Das erfordert, neben der klassischen E-Mail, ein breites Spektrum von Kommunikationsinstrumenten – von Chat über Video-Chat/-Konferenzen und Workflows bis hin zur sicheren Zusammenarbeit in den Dokumenten. Ohne entsprechende Kontrollen sind Sicherheit und Compliance gefährdet, und letztlich sind die IT-Abteilungen dafür verantwortlich. Unternehmen müssen sich überlegen, in welcher Form Cloud-Technologie und standardisierte Collaboration-Lösungen die erforderliche Kontrolle und Handhabung vertraulicher Informationen sowohl innerhalb als auch über die Firewall hinaus sicherstellen können.

### Individuelle Anforderungen

Standardisierte Dienste sollen an die unternehmenseigene IT-Infrastruktur, z.B. den Verzeichnisdienst, angebunden werden. Hier bieten die meisten CSPs einen sicheren Durchgriff auf das lokale Active Directory oder LDAP. Darüber erfolgt die automatisierte Provisionierung oder Löschung von Nutzern im Cloud-Dienst. Mithilfe von Plattform-as-a-Service (PaaS) lassen sich individuelle geschäftliche Anwendungskomponenten entwickeln. Dabei können SaaS-Komponenten verschiedener Anbieter über einen Internet-Service-Bus kombiniert werden. Unternehmen können ihre eigenen Anwendungen für die interne oder externe Verwendung entwickeln und in einer skalierbaren Cloud-Infrastruktur hosten. Dies ermöglicht eine schnellere und einfachere Entwicklung und bedeutet praktisch keinerlei laufende Wartung und schafft Skalierungsmöglichkeiten, mit denen Kapazitätsanforderungen kurzfristig gedeckt werden können. PaaS bietet über standardisierte Schnittstellen die Integration und Interoperabilität mit verschiedenen Technologieplattformen an. Je nach Hersteller existieren hier Services für Zugriffskontrolle und Prozess-Steuerung, Datenbankfunktionalitäten sowie für die Synchronisation von Anwendungen und Endgeräten in vernetzten Systemen. Für die modulare Nutzung von höherwertigen Services (PaaS, SaaS) innerhalb einer Anwendungsarchitektur ist das Architekturkonzept der verteilten, losen Kopplung im Sinne des SOA-Paradigmas eine grundlegende Voraussetzung.

### Michael Herkens

Geschäftsführer  
CLOUDPILOTS Software & Consulting GmbH  
E-Mail: michael.herkens@cloudpilots.com