DER HIMMEL VOLLER DATEN

Darum ist Cloud Computing der Speicherplatz der Zukunft

COLLENDA

Cloud Computing im Wandel der Jahre

Als die Idee des Cloud Computings geboren wurde, sahen IT-Departments noch aus wie die Kulisse aus einem James Bond-Klassiker. Klobige Mainframe-Maschinen mit der Leistungskraft heutiger Taschenrechner füllten die Räumlichkeiten. Wissenschaftler in weißen Kitteln und Maßanzügen programmierten darauf die ersten Anwendungen. IBM-Mitarbeiter Dr. Herbert R. J. Grosch war einer dieser Pioniere. Der 1910 geborene Kanadier arbeitete bereits in den 1950er Jahren am sogenannten Time-Sharing-Verfahren, das Zugriff auf den Großrechner von mehreren Terminals erlauben sollte. Die Ur-Idee des Cloud Computings war erdacht.

Und heute, über 60 Jahre danach? Der Speicherplatz in der Wolke ist sowohl im Privat- als auch im Unternehmensbereich längst etabliert. Das belegen auch die Zahlen: 35 Prozent der deutschen Bevölkerung im Alter zwischen 16 und 74 Jahren nutzen nach aktueller Angabe der europäischen Statistik-Behörde Eurostat Cloud-Dienste, um dort Dateien zu speichern – Tendenz steigend. Die Deutschen liegen damit exakt im europäischen Durchschnitt. In die Cloud werden Bilder geschoben, Programme wie Google Docs oder Microsoft 365 genutzt oder Backups von Smartphone oder PC gemacht. Der Zugriff ist von jedem Ort aus möglich.

In der Businesswelt hat sich die Nutzung der Cloud bisher insbesondere bei großen Unternehmen durchgesetzt. 62 % aller Unternehmen in Deutschland mit 250 oder mehr Mitarbeitern beziehen nach Angaben des Statistischen Bundesamts Cloud-Dienste (*Stand: Januar 2021*). Besonders häufig würden Services für die Speicherung von Daten (60 %), E-Mail-Dienste (56 %) und Office-Anwendungen wie Textverarbeitung oder Tabellenkalkulation (47 %) genutzt. Diese Zahlen, das ist jetzt schon klar, werden in den kommenden Jahren deutlich zulegen. Denn eines hat spätestens Corona offengelegt: Unternehmen, die die Digitalisierung vor der Pandemie vorangetrieben haben, haben in diesen schwierigen Zeiten einen entscheidenden Vorteil.

Unternehmen mit Bezug kostenpflichtiger IT-Dienste als Cloud Services	Beschäftigte		
	10 - 49	50 - 249	> 250
	Anteil **in %** an **allen Unternehmen**		
Insgesamt	31	41	62
E-Mail	57	54	50
Office-Anwendungen	45	52	55
Unternehmensdatenbanken	36	39	39
Speicherung von Dateien	65	68	67
Softwareanwendungen Finanzwesen	40	36	27
CRM-Software	18	23	30
Rechenkapazität eigene Software	20	24	36

Tabelle 1: Nutzung von Cloud Computing (Quelle: Statistisches Bundesamt)

Vorteile von Cloud Services

Die Vorteile des Cloud Computings liegen auf der Hand: Daten und Anwendungen sind online von jedem Ort aus abrufbar. Standardisierte Leistungen sind weniger fehleranfällig und können schneller und zu einem günstigeren Preis angeboten werden, als es viele Unternehmen mit ihrer internen IT umsetzen könnten. Auch bei der Implementierung hat das Cloud Computing einen entscheidenden Vorteil gegenüber On-Premises-Lösungen: die Geschwindigkeit. Rechenleistung und Speicherplatz können per Knopfdruck gebucht und sofort genutzt werden, ohne, dass die

unternehmenseigene IT-Abteilung Hardware anschaffen und einrichten muss. Dass Kapazitäten in der Cloud blitzschnell angepasst werden können, führt zudem zur einer stärkeren Kosteneffizienz.

Hinzu kommt: Insbesondere größere Unternehmen operieren in der Regel von mehreren Standorten aus. Daten und Anwendungen sind in der Cloud für alle Mitarbeiter verfügbar, unabhängig davon, wo sie sich befinden. Noch entscheidender ist dieser Faktor bei einer Expansion ins Ausland. Auch hier bietet der Daten-Himmel Vorteile, da Unternehmen ohne größere Startinvestitionen den Betrieb aufnehmen und flexibel auf Marktentwicklungen reagieren können. Verzögerungen wegen Zeitverschiebungen gibt es nicht mehr.

Cloud oder On-Premises? Eine Frage der Anforderungen.

Ist also eine Cloud-Lösung immer der Infrastruktur vor Ort vorzuziehen? Das pauschal zu beantworten ist schwierig und hängt von verschiedenen Faktoren ab. Ein Argument für die lokale Lösung kann sein, dass ältere Software in der Cloud nicht reibungslos läuft. Auch war in der Vergangenheit die fehlende Bandbreite des Internets ein Thema. On-Premises-Lösungen hatten hier durch geringere Latenzen die Nase vorn. Das ist heute völlig anders. Längst sind inzwischen die meisten privaten Haushalte mit sehr schnellen Internetverbindungen versorgt. Hinzu kommen spezielle Lösungen, die zum Beispiel über spezielle Schnittstellen Massendaten referenzieren und transportieren können.

Da sich der Kunde in der Cloud die Ressourcen in der Regel mit anderen Kunden teilt – sei es virtuell oder physisch –, muss das Thema Datenschutzgrundverordnung (DSGVO) natürlich ganz besonders im Fokus stehen. Jede Cloud-Lösung muss zwingend alle DSGVO-Vorgaben erfüllen!

Auch die Sicherheit von Geschäftsgeheimnissen – also das „Intellectual Property“ – ist für manches Unternehmen der Grund für die Wahl einer lokalen Lösung. Inzwischen sind jedoch viele Experten der Meinung, das Risiko in Cloud-Umgebungen sei ähnlich groß, wenn nicht sogar geringer. Sicherheitsabteilungen könnten in der Cloud schneller auf Cyber-Attacken reagieren und müsste nicht erst nach Fehlern in der eigenen Infrastruktur suchen. Die Wirtschaftsprüfungsgesellschaft KPMG stellt in ihrem „Cloud-Monitor 2020“ fest, dass zwar die Verdachtsfälle steigen, die Sicherheitsvorfälle jedoch abnehmen. Ein klares Indiz dafür, dass viele Cloud-Anbieter ihre Hausaufgaben beim Thema Sicherheit gemacht haben. In der Regel verfügen Cloud-Anbieter über eine höhere Sicherheitsexpertise als die interne IT-Abteilung vieler Unternehmen und bieten zeitgemäße und spezialisierte Tools zur Zugangs- und Schwachstellenkontrolle an.

Nicht zuletzt kann die Cloud im seltenen Fall einer Naturkatastrophe wie einem Brand oder einer Überschwemmung zum Datenretter für ein Unternehmen werden.

Arten von Cloud Services

- **Private Cloud:** Die IT-Infrastruktur wird dediziert für einen Nutzer bereitgestellt, zum Beispiel ein Unternehmen.
- **Public Cloud:** Hier erfolgt die Bereitstellung einer großen Infrastruktur für verschiedene Nutzer über das Internet. Es erfolgt eine virtuelle Trennung von Kundenumgebungen.
- **Community Cloud:** Ähnliche Institutionen werden in einer IT-Infrastruktur zusammengeschaltet.
- **Hybrid Cloud:** Eine Kombination verschiedenartiger Cloud-Strukturen, zum Beispiel eine Private Cloud mit Anteilen einer Public Cloud. Dem Kunden wird virtuelle Hardware dediziert bereitgestellt.

Maßnahmen für optimalen Schutz von Daten in der Cloud

Eine intelligente Sicherheitsarchitektur durch den Cloud-Anbieter ist dennoch natürlich unabdingbar, um einen optimalen Schutz der Daten zu gewährleisten. Das gilt insbesondere für Bereiche, in denen sensible Informationen durch die Datenkabel fließen. Dafür gilt es, auf unterschiedliche Sicherheit-Features zu achten.

- **Konfiguration der Cloud:** Eine sichere Konfiguration von Infrastruktur und Diensten ist der erste wichtige Schritt bei der Einrichtung der Cloud. Schon beim Deployment müssen die Dienste von Cloud-Anbietern bestimmten Kontrollen und Regulatorien genügen. Ein Indiz, dass Cloud-Anbieter die Sicherheit ernst nehmen, sind entsprechende Zertifizierungen.

- **Zertifizierung:** Audits wie zum Beispiel ISAE3402 oder ISO 27001 liefern den Nachweis, dass Unternehmen bestimmte Prozess- und Sicherheitsstandards in Segmenten wie zum Beispiel Berichtswesen, Incident und Change Management, Logical Access Management (Rollenberechtigungen und interne Prozesse) sowie General IT Controls erfüllen. Dabei gilt es zu beachten, dass sowohl Cloud-Anbieter, als zum Beispiel auch kooperierende Anbieter-Lösungen die entsprechende Zertifizierung erfüllen.

- **Datensicherung und Verschlüsselung:** Ein No-Brainer für jeden seriösen IT-Fachmann: Essentiell sind regelmäßige Datensicherungen. Sie sollten sowohl vom Cloud-Betreibers als auch vom Nutzer durchgeführt werden. Im Falle eines Datenverlusts oder eines verhinderten Zugriffs auf die Daten ist dadurch stets eine Notlösung gewährleistet. Zudem sollten Daten auf Festplatten, Backupmedien und in Datenbanken stets verschlüsselt abgelegt werden. Auch im Transit müssen diese Daten durch die Verwendung z. B. von HTTPS und SFTP Ende-zu-Ende verschlüsselt werden.

- **Zugriffsbeschränkung:** Zugriffe auf die Cloud von außen können auf eine bestimmte IP-Range oder per Site-to-Site-VPN eingeschränkt werden: die IP-Range erteilt im Vorfeld

nur bestimmten IP-Adressen die Zugriffsmöglichkeit; VPN bedeutet Virtual Private Network, in dem nur Partner, die dem Netzwerk angehören, miteinander verschlüsselt in Verbindung stehen. Das Site-to-Site-VPN beschreibt in der Regel eine Verbindung von Niederlassungsnetzwerken mit dem Netzwerk der Firmenzentrale. Beide Optionen sperren nicht autorisierte Nutzergruppen schlichtweg aus.

- **Trennung von Aufgaben- und Verantwortungsbereichen:** Die Verwaltung der Zugriffsrechte muss Unbefugten den Datenzugang verwehren. Der Zugriff sollte nach dem Grundsatz „Kenntnis nur, wenn nötig" gestattet werden. Dafür gilt es, die Verwaltung der Benutzerrechte zu organisieren, regelmäßig zu überprüfen und zu protokollieren. Klassifizierte Informationen werden von öffentlichen Informationen getrennt und die Zugriffsrechte nach dem Least-privilege-Prinzip vergeben.

- **DSGVO-Konformität:** Beim Thema Datenschutzgrundverordnung (DSGVO) sind sowohl Cloud-Betreiber als auch Cloud-Nutzer in der Pflicht. So ist zum Beispiel ein Server-Standort in Deutschland oder Europa ein Relevanzfaktor für DSGVO-Konformität. Für eine fehlerfreie Umsetzung sollte im Zweifelsfall die Hilfe eines Datenschutzbeauftragten hinzugezogen werden.

- **Pentests:** Schwachstellen im Sicherheitsschirm sollten regelmäßig geprüft werden. Cloud-Nutzer können die Sicherheit mit sogenannten Pentests (Penetrationstests) auf den Prüfstand stellen. Dafür wird in der Regel ein externer Dienstleister beauftragt, der testweise die Server mit Spam flutet oder versucht, sich in die Systeme zu hacken. Darüber hinaus sollte natürlich ein kontinuierlicher Schutz der Infrastruktur erfolgen. Zum Beispiel durch physische, betriebliche und softwarebasierte Maßnahmen. So helfen etwa regelmäßige Docker-Image-Scans, Schwachstellen frühzeitig zu erkennen.

- **Branchenspezifika bei der Auslagerung von Daten:** In unterschiedlichen Branchen müssen unterschiedliche Regulatorien berücksichtigt werden. Im Bankenwesen fordert zum Beispiel die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bestimmte Zertifizierungen und Maßnahmen gemäß BAIT (Bankaufsichtliche Anforderungen an die IT) oder MaRisk (Mindestanforderungen an das Risikomanagement der Banken). Diese Anforderungen müssen vor der Auslagerung von Daten in die Cloud genauestens überprüft werden.

Auch in Zukunft wird das Cloud-Business zweifellos florieren. In der Regel sind die Dienstleister am Puls der Zeit: Diskutiert werden im Zuge steigender Gefahren durch Cyber-Attacken neue Maßnahmen zum Schutz sensibler Daten wie das Zero Trust-Konzept. Keinem Nutzer, der Zugriff auf Dienste oder Daten haben möchte, wird diesem Prinzip zufolge von vornherein vertraut. Jeder Zugriff soll individuell überprüft, kontrolliert und authentifiziert werden, unabhängig davon, ob es sich um einen Mitarbeiter oder Kunden handelt. Private Apps aus dem Internet werden unsichtbar gemacht und ausschließlich autorisierten Nutzern der Zugriff auf die notwendigen Anwendungen gewährt.

Weitere Informationen zu unseren Lösungen

Über Collenda

Collenda ist ein führender Anbieter von Kreditmanagement- und Inkassosoftware für Banken, Unternehmen und Inkassobüros in ganz Europa. Durch weitreichende Erfahrungen in der Industrie bietet Collenda eine Cloud-fähige Suite von Anwendungen für die Verwaltung von Verbraucher- und Handelskrediten, mit deren Hilfe der gesamte Kreditlebenszyklus von der ersten Anfrage bis zur endgültigen Zahlung automatisiert werden kann. Intelligente Workflows, der Einsatz künstlicher Intelligenz und nutzerfreundliche Self-Service-Apps bieten einen effizienten und fairen Umgang mit jedem Kredit und gewährleisten das beste Ergebnis für die Gläubiger und ihre Kunden.