it-safe: Achten Sie gerade jetzt auf Cybersicherheit!

Cloud Anwendungen für kleine Unternehmen

Optimale Ergänzung oder Sicherheitsrisiko?

Stand: 14.05.2018

Cloud Computing, also die Nutzung verschiedener IT-Dienstleistungen über das Internet, ist inzwischen gut etabliert und wird in verschiedenen Formen angeboten. Gerade Klein- und Mittelbetriebe können Kostenersparnisse und oft auch Sicherheitsvorteile erzielen. Zuvor müssen allerdings zentrale Fragen, unter anderem im Sicherheitsbereich, geklärt werden.

Arten von Cloud-Anwendungen

Bei Cloud Computing können Unternehmen und Privatpersonen IT-Ressourcen oder Anwendungsdienste eines Service-Anbieters verwenden. Je nach Cloud-Modell werden bloße Infrastruktur (Rechenleistung, Speicherplatz, Netzwerkanbindung), Plattformen (Betriebssysteme, Web-Umgebungen) oder fertige Anwendungen (z.B. für ERP, CRM und BI, aber auch für Office- und E-Mail-Anwendungen) bereitgestellt. Diese Dienste werden vom Service-Anbieter ortsunabhängig und virtualisiert betrieben. Sie können von jedem Ort aus genutzt werden.

Für KMU ist es damit häufig möglich, ihre einfachen IT-Anforderungen – wenn z.B. ausschließlich Office-Programme und E-Mail sowie eine einfache Buchhaltung betrieben werden –vollständig über einen Cloud-Anbieter abzuwickeln und auf eigene Server zu verzichten. Auch die Ortsunabhängigkeit ist dabei von Vorteil, da auch im Außeneinsatz oder von zuhause auf die Cloud-Dienste zugegriffen werden kann.

Vorteile der Cloud – Immer up-to-date!

- Kostenersparnisse bei Investitionen sowie unter Umständen bei laufenden Kosten
- Entlastung oder Einsparung einer eigenen IT-Abteilung
- Elastizität und Skalierbarkeit, da zusätzliche Dienstleistungen kurzfristig zugekauft werden können und auch die Leistung flexibel angepasst werden kann
- Geschwindigkeitsvorteile, insbesondere gegenüber veralteter eigener Hardware
- Höhere Verfügbarkeit im Vergleich zu einem eigenen, kleinen Rechenzentrum

Risiken der Cloud – Wo sind meine Daten?

- Anbieterabhängigkeit, vor allem beim Wechsel zu einem anderen Service-Anbieter (Lock-in-Effekt), aber auch bei Support und Fehlerbehebung
- Verlust der Kontrolle über Daten und Prozesse sowie mangelnde Transparenz
- Leistungsstörungen (z.B. Einstellung der Leistung bei Zahlungsverzug)
- Lizenzfragen
- Schwierige Rechtsdurchsetzung gegenüber ausländischen Cloud-Anbietern (insb. in Drittstaaten)
- Und vor allem auch Risiken in den Bereichen Datenschutz und IT-Sicherheit

Unternehmen, die den Umstieg auf Cloud Computing planen, müssen sich des Risikos bewusst sein, dass in der Cloud die Daten und IT-Ressourcen geographisch verteilt sind. Cloud-Nutzerinnen und -Nutzer haben daher oft keine Ahnung, wo sich ihre Daten befinden und ihre Dienstleistungen erbracht werden.

US-Cloud-Lösungen & Datenschutz

US-Unternehmen haben unter dem „EU-US-Privacy Shield"-Abkommen die Möglichkeit, sich in eine vom US-Handelsministerium geführten Liste („Privacy Shield List") eintragen zu lassen, wenn sie sich zur Einhaltung der vereinbarten verbindlichen Datenschutz-Anforderungen gegenüber dem US-Handelsministerium verpflichten. Dadurch ist der Datentransfer in die USA wieder einfacher und ohne vorherige Genehmigung zu handhaben.

Heikle Daten in der Cloud

Bedenken Sie jedenfalls, dass die Verarbeitung sogenannter sensibler Daten (personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person) besonders heikel ist.

Aber auch bei nicht Daten, die zwar nicht personenbezogenen sind aber dennoch einen hohen Grad an Vertraulichkeit und Integrität erfordern – wie z.B. Rezepturen und andere Geschäftsgeheimnisse, Forschungsdaten u.Ä. –, sollten sich Cloud-Nutzerinnen und -Nutzer überlegen, ob diese Daten wirklich in einer Cloud-Umgebung verwendet werden sollen. Die Verarbeitung von personenbezogenen Daten sowie von Daten, die einen hohen Grad an Vertraulichkeit und Integrität erfordern, ist jedenfalls nur dann in einer Cloud nur zu verantworten, wenn der Anbieter genau darlegt, wie seine „Internet-Wolke" im Detail aufgebaut ist.

Daten in Österreich speichern - Gütesiegel Austrian Cloud

Das Gütesiegel „Austrian Cloud" ermöglicht Anbietern österreichischer Cloud-Lösungen explizit darauf hinzuweisen, dass sie die Daten in Österreich speichern. Den Anwendern erleichtert das Gütesiegel die Suche nach Unternehmen mit einem Speicherort im Inland!

» Weitere Infos