Kolumne Netzwerk Südbaden Ausgabe August 2019

Mit Sicherheit in die Cloud

KMU SEHEN NACH WIE VOR SICHERHEITSBEDENKEN ALS GRÖSSTES HEMMNIS FÜR EINE CLOUD-STRATEGIE – ZU RECHT?

Deutsche KMU haben die Vorteile der Nutzung von Cloud-Technologien als Triebfeder der Digitalisierung längst erkannt. Viele fürchten jedoch, beim Übergang in die Wolke die Kontrolle über wertvolle und sensible Daten zu verlieren. Zusätzlich stellen regulatorische Anforderungen des Gesetzgebers (z.B. DSGVO) oder Compliance-Anforderungen aus vertraglichen Verpflichtungen KMU vor große Herausforderungen.

Cloud-Dienste sind jedoch nicht per se mit einem niedrigen Sicherheitsniveau verbunden. Im Gegenteil: werden sie durchdacht eingesetzt, kann ein sehr hohes Maß an Datensicherheit erreicht werden. Bei weltweit agierenden Cloud-Providern wird beispielsweise über global verteilte Rechenzentren effizient eine optimale Systemredundanz und Verfügbarkeit erreicht. Skaleneffekte ermöglichen die kostengünstige Nutzung ausgereifter und belastbarer Sicherheitstools und -lösungen, deren Implementierung im eigenen Rechenzentrum nur mit extrem hohem Aufwand zu bewerkstelligen wäre.

Was gilt es also zu beachten, wenn Unternehmen die Vorteile der Cloud bestmöglich nutzen wollen, ohne zugleich Abstriche in puncto Sicherheit hinzunehmen?

Im Vorfeld sind die Anforderungen des Unternehmens an die Datensicherheit genau zu definieren. Ziel ist es, festzulegen, welche Art von Daten mit welchem Schutzbedarf in der Cloud verarbeitet werden sollen.

Folgende Fragen stehen daher am Anfang der Entwicklung einer unternehmensindividuellen Cloud-Strategie und eines stufenweisen Implementierungsplanes:

- Sind sensible Daten vor der Verarbeitung in der Cloud zu anonymisieren?
- Müssen Daten verschlüsselt gespeichert werden?
- Ist sichergestellt, dass jegliche Kommunikation mit den Cloud Diensten (via Internet) stets verschlüsselt erfolgt?
- Wie kann eine sichere Authentifizierung erfolgen, idealerweise gegen ein bereits bestehendes System?

Große Cloud-Anbieter warten häufig mit langen Listen von Zertifizierungen auf. Unternehmen sollten bei der Auswahl des Anbieters daher genau prüfen, welche Bereiche, Komponenten und Dienste die jeweiligen Sicherheitszertifikate abdecken (Scope) und ob dies den zuvor festgelegten Anforderungen Genüge tut.

Auch ist der Cloud-Provider oft nur für die Sicherheit der grundlegenden Infrastrukturkomponenten, wie beispielsweise dem Rechenzentrum, verantwortlich. Ein Großteil der Verantwortung in Bezug auf das gesamte Setup und den laufenden Betrieb verbleibt jedoch beim Kunden selbst.

Fazit:
Auf die Frage, ob Cloud-Lösungen sicher sind, gibt es keine allgemeingültige Antwort. Bei sorgfältiger Planung und intelligenter Nutzung von Cloud-Komponenten kann das Sicherheitsniveau einen sehr hohen Level erreichen. Ist intern kein eigenes Cloud-Knowhow verfügbar, empfiehlt es sich, sogenannte Managed Cloud Services zu beziehen. Neben professioneller Beratung hilft der Managed Cloud Provider dem Kunden dabei, die Möglichkeiten der Cloud optimal auszuschöpfen. Er kümmert sich um klassische technische Aufgaben wie Sicherheits-Updates und -Patches und bietet kompetenten Support rund um die Uhr.

Die Freiburger Continum AG versteht sich als Anwalt des Kunden und unterstützt Unternehmen auf dem sicheren Weg in die Cloud. Der zertifizierte AWS-Partner betreibt eigene Rechenzentren in Deutschland und erfüllt seit Jahren die Anforderungen der IT-Sicherheitsstandards PCI-DSS und ISO/IEC 27001. Die Continum AG ist einer der wenigen IT-Dienstleister in Baden-Württemberg, die hybride Cloud-Lösungen anbieten können. Kunden profitieren von dem sichersten und kostengünstigsten Weg in die Cloud, den erfahrenen Spezialisten bedarfsgerecht und individuell ausarbeiten.