Sicherheit von Anfang an – Multi-Cloud richtig gedacht

Multi-Cloud bringt Flexibilität – aber auch neue Risiken. Wer digitale Souveränität, Transparenz und Innovationskraft verbinden will, muss Sicherheit frühzeitig mitdenken. Denn eine starke Architektur beginnt nicht im Betrieb, sondern beim Design.

In der modernen IT-Landschaft stellt sich längst nicht mehr die Frage, ob Unternehmen die Cloud nutzen, sondern wie. Die Realität in vielen Schweizer Unternehmen ist heute bereits die Multi-Cloud. Dabei prägen individuelle Prioritäten die Cloud-Strategie: Manche Organisationen legen den Fokus auf Kontrolle und Schutz, andere auf Agilität und Technologievielfalt. Dieses Spannungsfeld zwischen Datensouveränität und globaler Innovationskraft macht Security by Design von Beginn an zur Pflicht. Denn: Eine robuste Multi-Cloud-Strategie basiert nicht auf Tools, sondern auf Prinzipien und mutigen Architekturentscheidungen.

Zwischen Flexibilität und Kontrolle

Insbesondere regulierte Branchen (Finanzwesen, Gesundheitssektor, Verwaltung) setzen auf Cloud-Modelle, die vollständige Kontrolle über Daten und Betrieb bieten. Lokale Private-Cloud-Anbieter ermöglichen Datenresidenz, Personalbindung im Inland und volle rechtliche Transparenz. Entscheidend ist dabei das Prinzip der digitalen Souveränität: zu wissen, wo die Daten liegen, wer sie verarbeitet und unter welchen gesetzlichen Rahmenbedingungen. Auf der anderen Seite bieten die Hyperscaler Zugang zu modernsten Technologien – von KI bis hin zur globalen Skalierung. Für innovationsgetriebene Unternehmen sind diese Plattformen sehr attraktiv, da sie neben Geschwindigkeit und Vielfalt der Dienste auch von den Milliardeninvestitionen dieser Anbieter in ihre eigene Sicherheit profitieren. Viele Unternehmen entscheiden sich jedoch für das Beste aus beiden Welten und setzen auf hybride Multi-Cloud-Architekturen. Doch je komplexer die Landschaft, desto höher das Risiko. Deshalb gehören Sicherheitsüberlegungen in die Strategie – und nicht erst in den Betrieb.

Der Weg zur sicheren Multi-Cloud

Die Zukunft der Unternehmens-IT ist hybrid und verteilt. Wer davon profitieren will, muss frühzeitig die richtigen Leitlinien setzen. Das heisst: Sicherheit ist kein Projekt, sondern eine Strategie, die vom ersten Architekturdiagramm bis zum produktiven Betrieb durchdekliniert werden muss.

Multi-Cloud ist kein Widerspruch zur Kontrolle – im Gegenteil: Mit einem starken Identity Management, durchdachter Governance, konsequenter Automatisierung und Security by Design wird aus Komplexität eine beherrschbare Stärke.

i FÜNF GRUNDPFEILER SICHERER MULTI-CLOUD

- **Starkes IAM:** In verteilten Cloud-Umgebungen wird die Identität zum Sicherheitsperimeter. Ein integriertes Identity- und Access-Management (IAM) mit Multi-Faktor-Authentifizierung und rollenbasierter Zugriffskontrolle ist der entscheidende «Klebstoff», der die Umgebungen sicher verbindet.
- **Einheitliche Governance und Automatisierung:** Sicherheitsrichtlinien, Konfigurationen und Compliance-Vorgaben müssen nicht nur definiert, sondern auch automatisiert durchgesetzt werden – cloudübergreifend und bei allen Umgebungen.
- **Transparenz durch Observability:** Ein zentralisiertes Monitoring mit Logs, Traces und Metriken schafft über alle Plattformen hinweg Transparenz und bildet die Basis für schnelle Incident Response und kontinuierliche Verbesserung.
- **Nachhaltiges Datenmanagement:** Der Schutz, die Portabilität und die Verschlüsselung sensibler Daten müssen über Cloud-Grenzen hinweg einheitlich geregelt sein. Dies gilt besonders für Daten in Transit sowie im Ruhezustand – und erfordert durchdachte Schlüsselverwaltungsprozesse.
- **FinOps und Kostenkontrolle:** Sicherheit braucht Ressourcen. Ein intelligentes Kosten- und Ressourcenmanagement sorgt dafür, dass Investitionen zielgerichtet und nachvollziehbar sind – ohne böse Überraschungen.

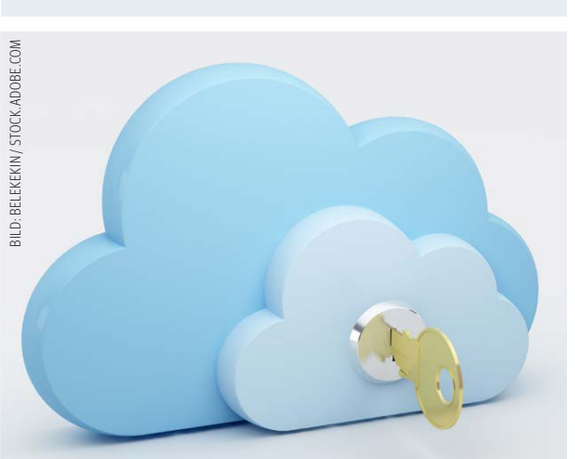

BILD: BELEKEKIN / STOCK.ADOBE.COM

DER AUTOR

Benjamin Kohler
Director Cloud Infrastructures, Convotis Schweiz

Den Beitrag finden Sie auch online
www.netzwoche.ch