## Die sichere Datenwolke

# Unterwegs in die Cloud

CIOs möchten die Vorteile von Cloud-Plattformen nutzen. CISOs sind hingegen skeptisch bezüglich der Risiko- und Governance-Auswirkungen. Wie stimmt man diese mit dem Unternehmensprofil ab?

→ VON MONIKA JOSI

Um Unklarheiten gegenüber der Sicherheit von Cloud-Lösungen zu beseitigen, sind ein systematisches Vorgehen und eine entsprechende Strategie erforderlich. Eine Übersicht über die wichtigsten Aspekte.

### 1 ENTWICKLUNG EINER CLOUD-STRATEGIE

Eine Cloud-Strategie wird aus der Perspektive des Unternehmens erstellt und beinhaltet nicht nur technische Aspekte. Eine umfassende Strategie berücksichtigt neben «lift-and-shift» auf Rechenzentrenstufe (IaaS) auch Überlegungen, welche Anwendungen durch PaaS- oder SaaS-Lösungen ersetzt, überarbeitet oder neu erstellt werden können. Zu berücksichtigen sind auch regulatorische, datenschutztechnische und andere sicherheitsrelevante Kriterien.

**Kernthemen:**

- Zu berücksichtigende Schutzanforderungen
- Sorgfältige Prüfung der Cloud-Strategie, abgestimmt auf die eigenen Anforderungen
- Überlegungen zur Vermeidung eines Vendor-Lock-ins und zur Sicherheit der Supply Chain

### 2 ENTWICKLUNG EINES GOVERNANCE-MODELLS

Basierend auf der Cloud-Strategie können Governance-Aspekte abgeleitet werden: Welche Auswirkungen haben die Modelle IaaS, PaaS oder SaaS auf die Governance? Welche Basiseinstellungen müssen berücksichtigt werden? Cloud-Provider bieten oft vordefinierte Blaupausen an, die es Kunden erleichtern, gewisse Standards in der gesamten Cloud-Umgebung zu setzen. Beispiele für zu definierende Aspekte sind einzuhaltende Standards und Normen wie ISO 27001, ISO 27017 oder auch ISO 27018. Hinzu kommen Governance der DevOps-Prozesse, Trennung von Ressourcen und Identitäten, Namensvorgaben, die geografische Region, in der Cloud-Resourcen betrieben werden, Umgang mit Datenschutzvorgaben, Security Logging, Monitoring etc.

**Kernthemen:**

- Verständnis des Shared-Responsibility-Modells entlang der Kette Provider – (Managed Provider) – Kunde
- Definition der Governance-Strukturen
- Abbildung der Compliance-Anforderungen
- Anwendbarkeit vordefinierter Standard-Templates

### 3 CLOUD-TRANSFORMATION

Bei der eigentlichen Transformation in die Cloud müssen die neuen Sicherheitsmöglichkeiten in der Cloud-Umgebung mitberücksichtigt werden. Eine Automatisierung der Prozesse verringert beispielsweise das Potenzial für Fehlmanipulationen. Unternehmen profitieren dabei von Sicherheitsmechanismen, die in der Cloud integriert sind.

**Kernthemen:**

- Container Security
- Evaluation von Security-Checks wie Multi-Faktor-Authentifizierung, Verschlüsselung und Schlüsselverwaltung, härtere Konfigurations-Settings, Least-Privilege-Ansätze
- Abdeckung der gesamten Sicherheitskette inklusive On-Premise, Hybrid- und Multi-Cloud
- Back-up-Anforderungen
- Transformation von Applikationen sowie von Cloud-ready-Anwendungen

### 4 CLOUD-BETRIEB

Ist die Cloud-Plattform in Betrieb, müssen die Sicherheitsmassnahmen zum Geschäftsrisiko passen. Wird eine Public-Cloud zur Unterstützung von Marketing- und Social-Networking-Initiativen verwendet, können Monitoring und Multi-Faktor-Authentifizierung ausreichen. Werden kritische Geschäftsfunktionen in die Cloud transferiert, sind zusätzliche Massnahmen zu prüfen, wie die Verwendung von Cloud Access Security Broker, detaillierte Schutzmassnahmen und Ende-zu-Ende-Verschlüsselung. Auch ist der «Security Incident Reponse»-Prozess zu definieren sowie die Rolle des Cloud-Providers und die Kontaktdetails im Notfall.

**Kernthemen:**

- Security Testing
- Security Logging und Monitoring, beispielsweise Security Information and Event Management und ein Security Operation Center in der Cloud
- Verschlüsselung inklusive Schlüsselverwaltung
- Identity und Access Management inklusive Privileged Account Management
- Sichere Konfiguration der Storage-Objekte
- Security-Incident-Response-Prozess

### FAZIT

Cloud Computing erfordert, dass Unternehmen einen Teil ihres Computing-Stacks in ein Shared-Responsibility-Modell überführen und dort pflegen. Das bietet die Chance, neue Ansätze und neue Methoden zum Schutz von Informationen zu prüfen und bisherige Schwachstellen durch die neuen Möglichkeiten zu adressieren und effizienter zu gestalten. Zudem fallen Sicherheitsprozesse weg, die den Unternehmen erfahrungsgemäss Schwierigkeiten bereiten, wie beispielsweise das zeitgerechte Patchen und die Aktualisierung von Versionen. ←

### DIE AUTORIN

**Monika Josi**
ist Head of IT-Consulting bei Avectris.
→ www.avectris.ch