Tipps für Datensicherheit in der Multi-Cloud

Die Nutzung von Cloudservices sollte umfassend geplant werden. Neben dem Faktor Performance hat auch die Datensicherheit mittlerweile geschäfts-kritische Relevanz erreicht. Regulatorische Standards sollten frühzeitig in das Multi-Cloud-Konzept einfließen, die Auswahl der Anbieter mitbestimmen und durch geeignete Maßnahmen flankiert werden.
Die Gründe für eine Multi-Cloud-Strategie sind vielfältig: Werden Services von mehreren Cloud Service-Providern genutzt, lassen sich Kosten einsparen, das Risiko von Anwendungsausfällen reduzieren und bestimmte Datenarten entsprechend regulatorischer Vorgaben innerhalb nationaler Grenzen speichern. Unternehmen legen Wert darauf, die jeweils am besten geeignete Plattform für bestimmte Prozesse zu wählen, Skalierbarkeit sicherzustellen und nicht ausschließlich von einem Anbieter abhängig zu sein. Da Multi-Cloud-Umgebungen eine größere Angriffsfläche für verschiedene Bedrohungen darstellen, gestaltet sich auch die Entwicklung einer geeigneten IT-Sicherheitsstrategie deutlich komplexer.
Damit potenzielle Sicherheitslücken gar nicht erst entstehen, sollte eine übergreifende Top-Down-Security-Strategie implementiert werden. Um eine Multi-Cloud-Umgebung erfolgreich zu verwalten und sicherzustellen, dass ein einheitlicher Sicherheits-status gewährleistet ist, sollte zunächst überprüft werden, wie Daten, Anwendungen und Workflows zwischen Cloud-Diensten und den verbundenen Geräten zusammenhängen. Daraus können die erforderlichen Maßnahmen abgeleitet werden, um die Datensicherheit zu gewährleisten.
Die folgenden fünf Tipps können Unternehmen dabei unterstützen, eine Sicherheitsstrategie zu entwickeln, die potenziellen Herausforderungen von Multi-Cloud-Umgebungen gewachsen ist:

1. Kontrolle über alle Unternehmensdaten gewinnen

Die Fähigkeit, Einblick in jede Cloud-Instanz zu haben, ist von entscheidender Bedeutung, um ungewöhnliche Verhaltensweisen zu identifizieren und den Datenverkehr während des Betriebs im Netzwerk zu überwachen.
Mit der Einführung weiterer Cloud-Dienste wird die Überwachung dieser Datenströme exponentiell schwieriger, aber auch unerlässlich. Unternehmen müssen darauf vertrauen können, dass sie Geräte und Daten - in einer sich ständig verändernden Umgebung – verfolgen, Richtlinien anwenden und pflegen können, wenn sich die Dinge im Laufe der Zeit ändern.
Wichtige Funktionen sind hierbei:
- Anwendungsübergreifende Aktivitätsprotokolle
- Verschlüsselung
- Kontrolle über Schatten-IT

2. Geeignete Identitäts- und Autorisierungskontrollen nutzen

Viele Unternehmen machen den Fehler, davon auszugehen, dass die Sicherheit bei der Ausführung ihrer Workloads in der Cloud in der alleinigen Verantwortung des Cloud-Anbieters liegt. Während Cloud-Provider für die Bereitstellung bestimmter Sicherheits- und Datenschutzniveaus in ihren Angeboten verantwortlich sind, liegt die Verantwortung für die Kontrolle, wer auf diese Daten zugreifen darf, beim Unternehmen.
Dies bedeutet, dass das Unternehmen über geeignete Tools verfügen muss, um sich vor Bedrohungen wie kompromittierten Anmeldeinformationen und bösartigen Insidern zu schützen. Folglich müssen Unternehmen wissen, wo sich ihre Daten befinden, wohin sie gehen und wer berechtigt ist, auf sie zuzugreifen. Mit robusten Authentifizierungsfunktionen legen Unternehmen einen wichtigen Grundstein für ihre IT-Sicherheit.
Erforderliche Kontrollmechanismen zur Unterstützung sind:
- Verhinderung der Datenexfiltration von einem genehmigten - zu einem nicht genehmigten Cloud-Service.
- Authentifizierung von Benutzern in allen Cloud-Anwendungen.
- Erkennung von Anomalien bei der Benutzeranmeldung.

3. Datenschutz während der Übertragung der Daten
Um Datenverlust in Multi-Cloud-Umgebungen vorzubeugen, benötigen Unternehmen leistungsstarke, Cloud-basierte Tools, die die Kontrolle über den Datenzugriff ermöglichen, das Online-Verhalten der Benutzer in Echtzeit überwachen, den Zugriff von nicht-verwalteten Endgeräte regeln und die Dateifreigabe steuern können.

Folgende Funktionen sollten die Sicherheitstools bieten:
- Unterscheidung zwischen persönlichen und geschäftlichen Instanzen von Cloud-Anwendungen und entsprechende Durchsetzung verschiedener Richtlinien
- Kontextabhängige
- Data Loss Prevention (DLP)

4. Endpoint-Security
Da immer mehr Mitarbeiter mit ihren privaten Geräten auf Cloud-Ressourcen im Unternehmen zugreifen, steigt das Risiko eines Verlustes sensibler Daten exponentiell an. Um Benutzer und Unternehmen zu schützen, ist es wichtig, dass Unternehmen einen sicheren mobilen Zugriff der Mitarbeiter auf die benötigten Daten ermöglichen können.

Für Unternehmen, die Bring-Your-Own-Device (BYOD) eingeführt haben, lässt sich durch agentenlose Sicherheitslösungen mit geringem Verwaltungsaufwand ein hohes Sicherheitsniveau herstellen: Diese schützen Daten während des Zugriffs, nutzen Verschlüsselungstechnologien, nehmen erforderliche Geräteeinstellungen vor und ermöglichen im Fall von Verlust oder Diebstahl die Entfernung der Daten auf dem Gerät per Fernzugriff.

5. Interoperabilität zwischen sämtlichen Security-Tools
Um einen ausreichenden Daten- und Bedrohungsschutz, Transparenz und Zugriffssicherheit über die gesamte Cloud-Umgehung eines Unternehmens hinweg zu erzielen, müssen Unternehmen sicherstellen, dass sich die von ihnen eingesetzten Cloud-Sicherheitslösungen nahtlos ineinander und mit bestehenden Tools vor Ort integrieren lassen. Eine unzusammenhängende IT-Umgebung kann zu inkonsistenter Cybersicherheit und damit zu Schwachstellen führen.
Beispielsweise müssen Cloud-Sicherheitslösungen eine Erweiterung der lokalen DLP-Richtlinien auf die Cloud und die Integration mit SIEM-Tools (Security Information Management) für das Sicherheitsinformations- und Vorfallmanagement bieten.

Fazit:
Die erfolgreiche Umsetzung einer Multicloud-Strategie erfordert einen ganzheitlichen Sicherheitsansatz, der die Sicherheit sensibler Informationen in jeder Cloud-Anwendung und auf jedem Gerät gewährleistet – rund um die Uhr. Das bedeutet, dass Unternehmen Daten jenseits ihrer klassischen Infrastruktur verwalten und schützen müssen, um langfristig ihre Wettbewerbsfähigkeit zu stärken.