IT CONSULTING & ENGINEERING

CLOUD BACKUP

SPEZIFIKA / ANFORDERUNGEN / BEDROHUNGSSZENARIEN / BACKUP TOOLS / EVALUATION

Cloud Computing ist momentan eines der wichtigsten Themengebiete im IT Markt. Dabei wird der Backup Aspekt oft zunächst vergessen.

So muss beim Anbieter ein spezieller Backup Service gebucht werden, wenn die Standard SLAs nicht ausreichend sind. Oft möchte man über vorhandene Möglichkeiten hinausgehen und verschiedene Cloud Backup Optionen kombiniert einsetzen:

- **OPB: On-Premise Backup**
- **C2C: Cloud-to-Cloud Backup** innerhalb einer bestehenden Cloud
- **C2OC: Cloud-to-other-Cloud Backup** der Cloud Daten in eine andere Cloud
- **C2OP: Cloud-to-On Premise Backup** der Cloud Daten in die On Premise Backup Lösung
- **OP2C: On Premise-to-Cloud Backup** der On-Premise Daten in die Cloud

Ihr Nutzen

- Neutrale, objektive und herstellerunabhängige Empfehlungen
- Einbezug von firmenspezifischen Rahmenbedingungen und Vorgaben
- Gesamtheitlicher und breit abgestützter Ansatz
- Rasches und effizientes Vorgehen
- Evaluation einer optimal auf Ihre Anforderungen angestimmten Backup Cloud Lösung
- Umfangreiche und nachvollziehbare Entscheidungsgrundlagen

Mit einer Begleitung durch die In&Out AG legen Sie die Basis für einen effizienten, sicheren und auf Ihre Bedürfnisse zugeschnittenen Einsatz Ihrer Cloud Backup Lösung.

Kontaktieren Sie uns

Gerne erläutern wir Ihnen unser Vorgehen in einem persönlichen Gespräch:

Andreas Zallmann
CEO
Bereichsleiter Plattformen
andreas.zallmann@inout.ch

Cloud Backup Spezifika

Bei Cloud Lösungen sind bezüglich der Backups folgende Spezifika zu berücksichtigen:

- Der Cloud Anbieter bietet normalerweise per Default keine Backups an, sondern nur eine einfache Papierkorbfunktion, in der gelöschte Dateien z.B. für 30 Tage aufbewahrt werden, bevor sie unwiderruflich gelöscht werden.
- Das gleiche gilt für das Überschreiben von Daten, hier wird in der Regel eine bestimmte Anzahl von Versionen vorgehalten und alle älteren Änderungen werden gelöscht.
- Der Anbieter garantiert für die Verfügbarkeit der Daten gemäss der definierten SLAs. Dabei ist ein Datenverlust in aller Regel nicht ausgeschlossen.

Anforderungen an Cloud Backups

Neben den klassischen On-Prem Backups werden Cloud Backup-Lösungen aufgrund folgender Anforderungen notwendig:

- Der Kunde möchte eine echte Backup Lösung, die über Versionen und Papierkorbfunktion hinausgeht.
- Es sollen vom Anbieter abweichende Backup Policies (Sicherungszeitpunkt, Sicherungshäufigkeit, Backup Typ), sowie Aufbewahrungsfristen realisiert werden.
- Das Backup Angebot des Cloud Anbieters ist zu teuer.
- Der Kunde möchte das Backup ausserhalb der Cloud des Anbieters halten, damit bei einer grösseren Störung des Cloud Anbieters die Daten noch sicher verfügbar sind.
- Der Kunde möchte die Daten zusätzlich zur Cloud lokal On-premise halten, oft aus regulatorischen Erfordernissen, die beispielsweise vorsehen, dass die Daten jederzeit wieder zum Kunden zurückgeholt werden können.
- Der Kunde möchte ein zusätzliches Backup seiner On-Prem Daten in der Cloud halten.

Weitere Bedrohungsszenarien

Kombinierte Cloud-On-premise Backups werden eingesetzt, um spezifische heutige Bedrohungsszenarien zu adressieren:

- *Ransomware Protection*: Erweiterter Schutz vor Datenverschlüsselung, indem eine unabhängige Backup Kopie mit zusätzlichen Sicherungsmechanismen etabliert wird.
- *Ransomware Detection*: Kombination der Backup Lösung mit Ransomware Erkennung, indem z.B. mit KI oder regelbasiert gewisse Anomalien (z.B. ungewöhnliche Änderungshäufigkeiten) erkannt werden, die mögliche Anzeichen für einen Ransomware Befall sein können.
- *Bad Admin Protection*: Backup in eine andere Umgebung (andere Cloud, Cloud nach On-Premise oder On-Premise in Cloud) erlaubt eine bessere Trennung der Berechtigungen und der Verantwortung (Segregation of Duty) für die einzelnen Backups und die Originaldaten. Ziel ist es, die Manipulation oder Löschung von Daten und aller Backups durch Administratoren zu verhindern.

CLOUD BACKUP

SPEZIFIKA / ANFORDERUNGEN / BEDROHUNGSSZENARIEN / BACKUP TOOLS / EVALUATION

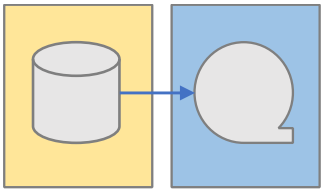
Cloud Backup Tools

- Bei Evaluationen von Backup Tools sollen verschiedene Backup Szenarien auch in der Cloud oder zwischen Cloud und On-Prem Installationen möglich sein. Dabei soll möglichst ein identisches Backup Tool zum Einsatz kommen, das möglichst viele dieser Szenarien abdeckt.
- Die aktuellen gängigen on-prem Backup Tools wie Veeam, Commvault, Netbackup, Networker, Spectrum Protect, Rubrik, Cohesity und andere bieten heute alle mehr oder weniger ausgeprägte Cloud Backup Funktionen, die oft auch applikationsspezifisch sind (z.B. Office 365, Sharepoint, etc.).

Cloud Backup Modelle

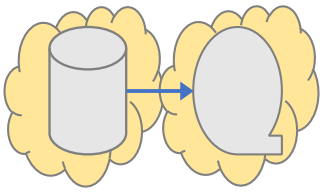
Nachfolgend sind die wichtigsten Cloud Backup-Modelle aufgeführt:

OPB: Klassisches On-Prem Backup



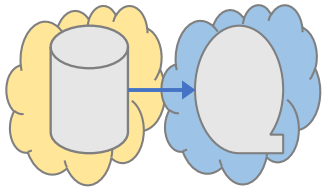
On-Prem Backup (OPB) ist das klassische Backup von Storage Daten in eine on-premise Backup Umgebung. In der Regel erfolgt der Backup in einen anderen Standort oder an mehrere Standorte der Kunden.

C2C: Cloud-to-Cloud Backup



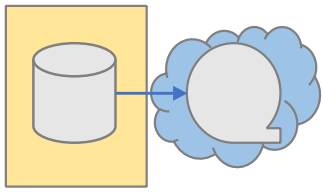
Cloud-to-Cloud Backups (C2C) sichern die Cloud basierten Daten auf eine Backupumgebung des gleichen Cloudanbieters (ggf. in eine andere Zone oder Region). Dabei kann der Kunde auch ein Cloud basiertes eigenes Backup Werkzeug einsetzen und die Sicherungs- und Aufbewahrungspolicies frei wählen.

C2OC: Cloud-to-other-Cloud Backup



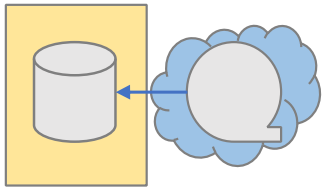
Cloud-to-other-Cloud Backups (C2OC) entsprechen C2C Backups zu einem anderen Cloud Provider und gewährleisten somit eine zusätzliche Unabhängigkeit vom eigentlichen Cloud Provider, der die primären Daten verwaltet.

OP2C: On-Prem-to-Cloud Backup



On-Prem-to- Cloud Backups (OP2C) sichern die lokalen on-premise Daten (in der Regel ergänzend zu lokalen Backups) in eine Cloud Umgebung, um eine zusätzliche unabhängige Kopie zu gewährleisten und einen zusätzlichen Schutz vor lokalen Katastrophen, Ransomware Attacken oder Bad Admin Szenarios zu gewährleisten.

C2OP: Cloud-to-On-Prem Backup



Cloud-to-On-Prem Backups (C2OP) sichern die cloudbasierten Daten zum on-premise Standort der Kunden, um damit einen weiteren Schutz zu gewährleisten, die Kontrolle über die Sicherungs- und Aufbewahrungspolicies zu erhalten und beispielsweise aus regulatorischen Gründen die Daten jedereit lokal zugreifbar zu haben.