Der Weg zur richtigen Backup-Strategie

Mit Sicherheit in die Cloud

Die Datensicherung mit ihren standardisierten und wiederkehrenden Tätigkeiten zählt zu den IT-Leistungen, die ein hohes Einsparpotenzial versprechen. Aufgaben rund um das Backup tragen nicht wirklich zur Wertschöpfung bei und rauben hochbezahlten IT-Spezialisten ihre kostbare Zeit – so die Meinung in vielen Chefetagen. Dies verführt viele Manager dazu, beim Backup gefährliche Kompromisse einzugehen. Die ständig wachsenden Datenmengen, die steigende Abhängigkeit der Unternehmen von ihren operativen Daten sowie die Vorschriften zur Datenarchivierung machen es jedoch notwendig, die Backup-Strategie kontinuierlich weiterzuentwickeln.

Geschäftsführer und IT-Manager sind sich bewusst, dass ihre Organisation in hohem Maße von der IT abhängt. So hat eine Umfrage der Initiative „Cloud Services Made in Germany" im deutschen Mittelstand ergeben, dass 95 Prozent der befragten Organisationen ohne Daten ihre Geschäftsprozesse nicht mehr in der gewohnten Weise ausführen können. Bei 51 Prozent der Unternehmen droht sogar ein vollständiger Stillstand der Organisation, wenn operative Daten nicht mehr zur Verfügung stehen.

Für die Geschäftsführung stellt sich die Frage, ob die immer wieder angeforderten IT-Investitionen für das Backup tatsächlich notwendig sind. Vor allem geht es darum, ob das Backup auch weiterhin in der vollen Fertigungstiefe selbst erbracht werden muss. Mit dem Einzug der Cloud in die Unternehmens-IT sowie ständig steigenden Netzwerkkapazitäten zu günstigen Preisen wird es immer naheliegender, Backup-Prozesse in die Cloud zu verlagern.

Warum sich die Auslagerung lohnt

Wer sich mit Backup-as-a-Service (BaaS) die Cloud ins Rechenzentrum holt, spart zunächst einmal die Investitionskosten für zusätzliche Storage-Kapazitäten im Backup-Umfeld. Zudem ist der Cloud-Speicher sehr flexibel und nach Bedarf buchbar. Die Nutzung der Cloud erhöht zudem die Sicherheit im Katastrophenfall. Wird zusätzlich zu einem Backup im eigenen Rechenzentrum die Cloud als Speicher genutzt, lassen sich nach einem Brand oder Wasserschaden die gesicherten Backup-Daten schnell wieder einspielen. Dazu ein Praxistipp: Die Themen Backup und Disaster Recovery (DR) werden häufig als zwei getrennte Technologien und Prozesse angesehen. Diese künstliche Trennung ist ineffizient, da es bereits zahlreiche Lösungen gibt, die beide Funktionen in nur einem Produkt kombinieren.

Um die Cloud-Dienste zu nutzen, wird eine leistungsfähige Internet-Anbindung benötigt. Der konkrete Bandbreitenbedarf ergibt sich aus den zu übertragenden Datenmengen und dem zur Verfügung stehenden Zeitfenster für die Datenübertragung. Wer auf Nummer sicher gehen möchte, verbindet das eigene Rechenzentrum über mehrere Netzanbieter mit der Cloud.

Den richtigen Anbieter finden

Unternehmen haben höchst individuelle Anforderungen an Sicherheit, Datenmengen und verfügbare Backup-Zeiten. Zudem möchten IT-Verantwortliche trotz Cloud-Integration ihre bereits getätigten Investitionen in Backup-Software und Storage-Systeme sichern. Wer daher einen Beratungs- und Implementierungspartner sucht, sollte sich von diesem zunächst Referenzprojekte vorstellen lassen, die dem eigenen Cloud-Projekt möglichst nahe kommen. Ein weiterer wichtiger Punkt: Der Cloud-Anbieter sollte ein Rechenzentrum in Deutschland betreiben und durch Auswahl des richtigen Providers sicherstellen, dass die Daten Deutschland nicht verlassen. Eine verschlüsselte Datenübertragung gilt als Standard.

So gelingt der Start

Bevor die Backup-Daten erstmalig in die Cloud übertragen werden, ist eine Analyse der Datenmengen und Übertragungskapazitäten notwendig. Im einfachsten Fall ist das Zeitfenster für das Backup ausreichend und die initiale Übertragung erfolgt bequem online und unter Verwendung der bestehenden Backup-Software. Ist das nicht möglich, gibt es Alternativen – beispielsweise die Speicherung der Initialdaten auf eine physische Storage-Einheit, die per Kurier zum Provider gelangt. Gute Berater bieten hier ganz unterschiedliche Leistungen für den Start in die Cloud, die sich immer an der beim Kunden vorhandenen IT-Infrastruktur orientieren.

Auch sollte die Backup-Lösung die Daten schon vor der Übertragung komprimieren

Vorteile des Backups als Cloud-Service. Quelle: NetApp

und deduplizieren. Die Funktionen hierfür sind in den meisten modernen Backup-Umgebungen bereits vorhanden. Weiterhin nutzen viele Anbieter heute dezidierte Appliances (physikalische oder virtuelle), um eine Brücke zwischen dem Rechenzentrum des Kunden und der eigenen Cloud-Infrastruktur zu bauen. NetApp beispielsweise hat hierfür im Mai 2015 die Lösung „AltaVault" (früher Steelstore) vorgestellt. Diese bietet unter anderem eine Inline-Deduplizierung und Komprimierung, wodurch eine hohe Datenreduktionsrate erreicht wird.

Was tun, wenn es brennt?

Beim Zurückspielen der Daten in die eigene IT-Infrastruktur ist zwischen Restore und Disaster Recovery (DR) zu unterscheiden. Ein Restore erfolgt nach entstandenem Datenverlust und innerhalb vereinbarter Service-Level. Hier ist also bekannt, wie lange die Wiederherstellung operativer Daten bei einer gegebenen Internet-Anbindung dauert. Bei einem DR muss dem Kunden in kürzester Zeit eine neue Infrastruktur zur Verfügung gestellt werden, damit das Unternehmen wieder operativ tätig werden kann. All diese und weitere Fragen fließen in eine übergreifende Backup-Strategie ein und sollten mit einem darauf spezialisierten Dienstleister erörtert werden. Grundsätzlich kann ein Unternehmen deutlich flexibler auf die unterschiedlichen Restore- und DR-Anforderungen eingehen, wenn die Daten erst einmal in der Cloud gesichert sind. Beispielsweise können im Notfall virtuelle Arbeitsplätze über die Cloud bereitgestellt werden, bis die lokalen PCs wieder betriebsbereit sind. Sind die Backup-Daten schon in der Cloud, erfolgt ein Restore oder DR sehr sicher innerhalb der vereinbarten Service-Level.

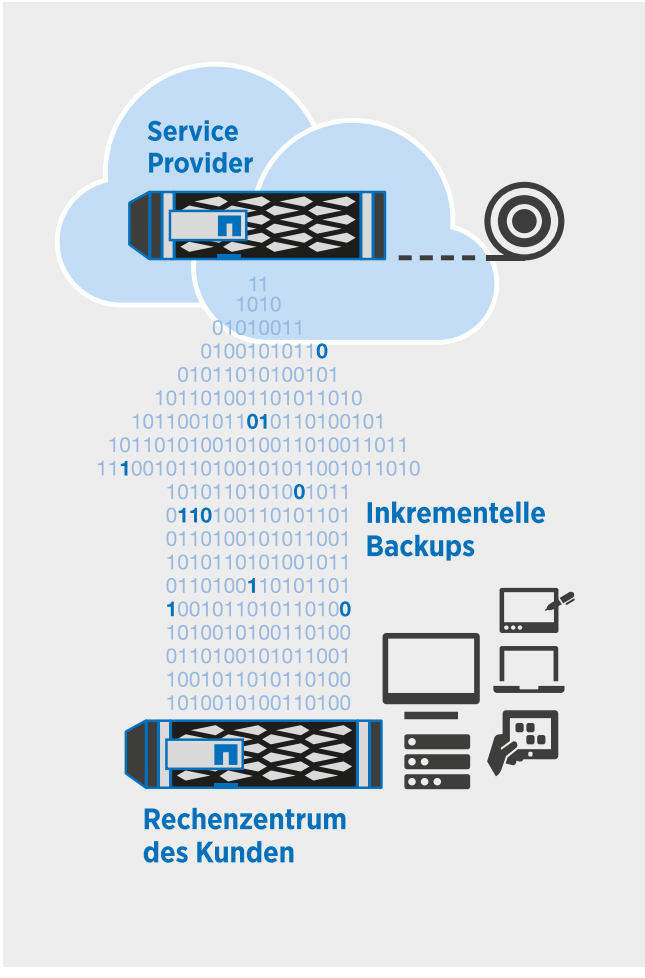
Sicherheitsaspekte

Die deutschen Datenschutzvorschriften verlangen, dass beispielsweise personenbezogene Daten den deutschen Rechtsraum nicht verlassen dürfen. Zwar gibt es heute bereits eine Vielzahl von BaaS-Angeboten in Deutschland, jedoch sind diese zum Teil nicht validiert und es fehlt ein einheitlicher Qualitätsstandard. Zudem ist es nicht selbstverständlich, dass Anbieter auch tatsächlich über ein Rechenzentrum in Deutschland verfügen.

Ein valides BaaS-Angebot sollte ausschließlich auf autorisierte Service Provider mit Rechenzentrum in Deutschland setzen und Nutzern die Möglichkeit bieten, Daten in die Cloud auszulagern und so die komplette Datensicherung als Leistung zu beziehen. Dinge wie ein Leistungsschein mit einer Zusammenfassung der vereinbarten Services und klarer Definition des Leistungsstandards sind hilfreich, um die Servicequalität zu sichern. Die eingesetzten Technologien sollten es erlauben, die Backup-Daten flexibel in die Cloud und wieder zurück zu kopieren. Die Cloud wird somit nicht zu einer Einbahnstraße und Kunden behalten jederzeit die volle Hoheit über ihre Daten.

Fazit

Ob intern oder extern – Datensicherung gehört in die Hände von IT-Profis, da die operativen Daten für den täglichen Geschäftsbetrieb enorm wichtig sind. Mit Backup-Services aus der Cloud erhalten Unternehmen heute eine sichere und praxiserprobte Lösung, um die eigene Backup-Strategie zu optimieren und die Effizienz im IT-Betrieb zu steigern. ■



Ein Full Backup ist vor allem beim Start in die Cloud notwendig. Im weiteren Verlauf reicht in der Regel ein inkrementelles Backup, bei dem erheblich weniger Daten übertragen werden.
Quelle: NetApp

Nützliche Links

- *BSI: IT-Grundschutz*
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- *BITKOM: Leitfaden Cloud Computing*
  https://www.bitkom.org/de/themen/61490.aspx
- *NetApp: BaaS*
  www.netapp.de/baas/

PETER WÜST,
Director Cloud & Alliances CEMA bei NetApp