BACKUP UND HOCHVERFÜGBARKEIT

WANN LOHNT DIE AUSLAGERUNG IN DIE CLOUD?

Wie lässt sich das *Daten-Backup* sicher und datenschutzkonform organisieren? Was bringt die Auslagerung des Backups in die Cloud? Inwieweit können Managed-Service-Provider dabei garantieren, dass die Daten auf deutschem Boden vorgehalten werden? Antworten auf diese und andere Fragen gibt *Udo Böhm,* Leiter Business Development bei der SHD System-Haus-Dresden GmbH.

ITM: *Herr Böhm, wie können mittelständische Kunden ihr Backup bestmöglich organisieren?*
UDO BÖHM: Gemäß der gängigen Backup-Faustregel „3-2-1" sollten mindestens drei Kopien der Datensicherung vorgehalten werden. Diese wiederum sollten auf mindestens zwei verschiedenen Datenträgern lagern. Dies bedeutet, dass außer auf der Festplatte des Sicherungssystems die Daten auch auf externen Festplatten, Tapes oder optischen Speichermedien liegen sollten. Mindestens eine dieser Kopien sollte man darüber hinaus außerhalb des Firmengebäudes lagern.

Eine Alternative zu physischen Speichermedien stellt dabei das Cloud-Backup dar, wobei auf Basis der 3-2-1-Regel vielfältige Sicherungsszenarien möglich sind. Dabei lässt sich grundsätzlich zwischen „Self-Service-Backup" und „Managed Backup" unterscheiden: Beim cloud-basierten Self-Service-Backup verwalten die Kunden ihre „Backup to Disk"-Umgebung weiterhin selbst und ersetzen etwa ihre Tape-Lösungen durch Cloud-Services. Dabei können sie auf Public-Cloud-Speicher beispielsweise von Amazon Web Services setzen oder ihre Daten in die Private Cloud eines Managed-Service-Providers übergeben.

ITM: *Welche Aufgaben übernehmen Managed-Service-Provider in der Regel?*
BÖHM: Sie können nicht nur verschiedene Backup-Szenarien realisieren, sondern auch die Übernahme des Backups und die Verantwortung für die Wiederherstellung der Daten gemäß definierter Service Level Agreements (SLAs) realisieren. Externe Dienstleister liefern fachliche Beratung und weitergehende Infrastrukturservices. Nicht zuletzt bieten sie ein kontinuierliches Monitoring der Backup-Ströme und regelmäßige Reporting-Berichte.

ITM: *Wie sollte man den Umstieg auf ein Cloud-Backup am besten angehen?*
BÖHM: Im Rahmen unserer Projekte starten wir stets mit einer umfangreichen Beratung, in deren Rahmen wir den Ist-Zustand bewerten. Gemeinsam mit den Kunden klären wir dabei u.a. folgende Fragen:

- Inwieweit ist das aktuelle Backup- und Restore-Konzept dokumentiert?
- Was kosten die bisherige Backup-Lösung und ihr Betrieb inklusive der Weiterbildung der Mitarbeiter sowie einer ausreichenden Personaldecke für den Krankheits- oder Urlaubsfall?
- Wie schnell können Daten wiederhergestellt werden? ›

- Welche Service-Level gelten an dieser Stelle?
- Wie sicher ist man, dass die Wiederherstellung von Daten technisch funktioniert und die Recovery Time Objective (RTO) genügt? Wurden in der Vergangenheit regelmäßige Restore-Tests durchgeführt?
- Inwieweit deckt das Backup-/Restore-Konzept auch die IT-Notfallplanung des Unternehmens ab?

Im nächsten Schritt definieren wir gemeinsam mit den Kunden die Anforderungen an ihre Backup-Lösung. Wir klären, ob man nur Backup-Services nutzen oder überdies auch eine Notfallplanung einbeziehen sollte.

ITM: *Was passiert beim Umstieg in die Cloud mit den bislang auf traditionellen Backup-Medien wie Disk oder Tape gespeicherten Daten?*
BÖHM: Es gibt Unternehmen, die die Verwaltung ihrer Firmendaten komplett ausgelagert haben. Das bedeutet, dass keine historischen Daten auf den Server-Systemen im Unternehmen vorliegen. Lokales Backup to Disk ist heute quasi ein Standard für die schnelle Wiederherstellung von Daten. Nur wenn der Speicher nicht groß genug ist, werden zumeist die Monats- und Jahres-Backups auf Tapes ausgelagert. Möchte man auf diese auch zukünftig zugreifen und in eine Cloud spielen, ist zunächst ein Import der Daten zurück ins Unternehmen notwendig. Dafür müssen dort entsprechende Speichersysteme vorhanden sein, die die bislang eingesetzten Backup-Technologien unterstützen können.

ITM: *Wer ist in mittelständischen Unternehmen für das Backup zuständig?*
BÖHM: Zumeist betrifft dies die Systemadministratoren, wobei Backup-Prozesse meist automatisiert im Hintergrund ablaufen. Allerdings müssen die Admins kontinuierlich überprüfen, ob die Backups tatsächlich auch fehlerfrei abgelaufen sind.

ITM: *Wie lassen sich Backup-Daten vor aktuellen Bedrohungen wie Ransomware schützen?*
BÖHM: Die Verantwortlichen sollten bereits auf Client-Seite alles dafür tun, dass sich Ransomware erst gar nicht im Unternehmen ausbreitet. Somit kann sich Ransomware auch nicht unter die Backup-Daten schummeln. Sollten dennoch Backup-Daten aufgrund einer Infizierung mit Ransomware verschlüsselt werden, ist nach der Beseitigung der Ursache eine Wiederherstellung der betroffenen Daten oft die bessere Alternative als die Zahlung von Lösegeldern.

KEINE ZAHLUNG VON LÖSEGELDERN

ITM: *Welche Rolle spielen Backup-Konzepte im Rahmen der ab Mai 2018 gültigen EU-Datenschutz-Grundverordnung (EU-DSGVO)?*
BÖHM: Prinzipiell spielt das Daten-Backup im Rahmen der EU-DSGVO eine eher untergeordnete Rolle. Wichtig ist jedoch, dass die Daten verschlüsselt an den Provider oder in die Cloud übertragen und dort auch verschlüsselt vorgehalten werden. Für Anwenderfirmen ist es sehr wichtig, ein Konzept für die Umsetzung der EU-DSGVO zu haben. Denn generell sind alle im Unternehmen vorhandenen personenbezogenen Daten davon betroffen. Das Problem dabei: Die Verwaltung personenbezogener Daten gestaltet sich recht komplex. In diesem Zusammenhang sollten vorgegebene Richtlinien verhindern, dass Daten kopiert oder missbraucht werden können.

Ab neun Mitarbeitern, die mit personenbezogenen Daten arbeiten, müssen die Unternehmen zudem einen Datenschutzverantwortlichen bestellen. Dabei können sie sich ihren Datenschutzverantwortlichen auch von externen IT-Dienstleistern „ausleihen".

ITM: *SHD selbst bietet verschiedene Infrastruktur-Services an, darunter auch sogenannte Cloud-Storage-Target-Lösungen. Was steckt dahinter?*
BÖHM: Im Allgemeinen versteht man unter „Cloud Storage" skalierbare und im Internet vorgehaltene Speicherinfrastrukturen. Diese sind via Self-Service-Portal erreichbar und in verschiedenen Preisklassen erhältlich. Klassischer Cloud-Objekt-Storage wird über besondere Schnittstellen von vielen Archiv- und Backup-Anbietern bereits im Standard bedient.

Wir bieten neben Objektspeicher auch individuelle Storage-Umgebungen in unserer privaten SHD-Cloud an. Hier können die Kunden eigene virtuelle Maschinen betreiben oder auch Archivspeicher beziehen. Dabei setzen unseren Lösungen u.a. auf Objektspeicher vom Hersteller Cloudian inklusive der Anbindung an die Amazon-S3-Schnittstelle oder auch auf Enterprise-professionelle Storage-Lösungen der Firma Netapp auf.

ITM: *Im Mittelstand herrschen mitunter noch immer Vorbehalte gegenüber Cloud-Lösungen. Wie wollen Sie Skeptiker von Ihren Cloud-Lösungen überzeugen?*
BÖHM: Mittelständische Unternehmen bevorzugen Partner auf Augenhöhe, die sich als „Dienstleister" der Kunden verstehen. Sprich: Diese müssen erreichbar sein und auch dann weiterhelfen, wenn etwas nicht explizit im Vertrag festgeschrieben wurde.

Funktionieren Backup-Prozesse bei weltweiten Public-Cloud-Anbietern nicht, müssen die Nutzer meist auf Englisch mit Mitarbeitern in Callcentern telefonieren. Wir hingegen sind zwar als lokaler Service-Provider zunächst hochpreisiger unterwegs als die Public-Cloud-Anbieter, bieten unseren Kunden jedoch direkten Support mit bekannten Mitarbeitern. Generell gestaltet sich der Bezug von IT-Services im Mittelstand stets als Vertrauensthema – und dafür zahlen die Kunden gerne etwas mehr.

INA SCHLÜCKER

> „Die Systemadministratoren sollten auch bei automatisierten Backup-Prozessen kontinuierlich überprüfen, ob sie tatsächlich auch fehlerfrei abgelaufen sind und zyklisch Restores testen",
>
> *betont* **Udo Böhm,** *Leiter Business Development bei SHD.*