Datenlöschung im Cloud-Zeitalter

Wo lagern unsere Unternehmensdaten? Wie werden sie verarbeitet? Und wie können sie wieder gelöscht werden? In Zeiten der Cloud verschwimmt die Sicht auf den Datenzyklus. Dabei ist genau diese entscheidend für den sicheren und hochverfügbaren Betrieb von Anwendungen.

→ **VON KASPAR GEISER**

Unsere Daten sind überall und nirgends. Dank Cloud Computing haben wir die Möglichkeit, von überallher und mit verschiedenen Geräten auf unsere Daten zuzugreifen. Ein Klick, und sie sind mit anderen Benutzern geteilt. Was aber, wenn wir sensitive Daten löschen wollen? Geht das überhaupt noch? Um die Antwort vorwegzunehmen: Es geht nur noch unter bestimmten Voraussetzungen. Nicht nur beim Löschen, sondern generell bei der Datensicherheit in der Cloud ist eine klare Sicht auf den gesamten Datenzyklus entscheidend – vom Schreiben und Erfassen über das Halten und die Backups bis zur allfälligen Löschung.

DATENKLASSIFIZIERUNG

Jeder muss sich Gedanken machen, wie stark seine Daten zu schützen sind – für jeden Geschäftsfall individuell. Schon vor dem Start eines Cloud-Computing- oder Outsourcing-Unterfangens müssen die Anforderungen an die Daten definiert sein. Die IT benutzt dafür die Begriffe Vertraulichkeit, Verfügbarkeit und Integrität. Mit der Vertraulichkeit sollen der Empfängerkreis und die Weitergabe geregelt werden. Die Verfügbarkeit definiert, über welchen Zeitraum pro Tag, Woche, Monat oder Jahr die Daten dem Anwender zur Verfügung stehen sollen. Die Integrität stellt die Anforderung an technische Systeme zur Erkennung von Veränderungen der Daten. Diese Anforderungen festzulegen, ist die Voraussetzung für die technische Umsetzung der Datenhaltung.

ÜBERTRAGUNG & VERARBEITUNG

Vor dem Speichern müssen Daten erfasst, übertragen und allenfalls verarbeitet werden. Damit die Daten beim Erfassen nicht in falsche Hände geraten, muss dies auf einem sicheren Rechner in einer sicheren Umgebung geschehen. Dies wiederum bedingt mindestens eine starke Authentisierung am Arbeitsgerät des Verfassers sowie in der betreffenden Anwendung, zum Beispiel dem Content-Management-System. In der Regel ist auch die physische Anwesenheit an einem Ort – zum Beispiel dem Büro – definiert.

Die Übertragung der Daten zum Serversystem kann auf verschiedene Arten geschützt werden. Zum Beispiel lassen sich dedizierte Leitungen zwischen Büro und Rechenzentrum mit darin integrierter Verschlüsselung (VPN) verwenden. Zwischen Browser und Anwendung wird zudem TLS (Transport Layer Security, vormals SSL) verwendet. TLS erschwert es potenziellen Mitlesern, Daten bei der Übertragung mitzulesen. Im Rechenzentrum angekommen, werden die Daten verarbeitet oder einfach abgelegt. Doch auch dieser Schritt erfordert höchste Aufmerksamkeit. Werden beispielsweise Daten vor der sicheren Speicherung in einer Datenbank zu einem PDF verarbeitet, entstehen dabei Logfiles. Diese Logfiles können selbst auch Inhalte bzw. Daten enthalten. Für eine sichere Datenverarbeitung gilt also: Logdateien einer Anwendung müssen denselben Anforderungen unterliegen wie die eigentlichen Daten.

BILD: ISTOCKPHOTO.COM/SHAWN_HEMPEL

LAGERUNG

Die grösste Herausforderung besteht in der Lagerung oder Speicherung der Daten. Daten können als Rohdaten in einem Dateisystem lagern oder als Einträge in einer Datenbank. Wer nun den Anspruch stellt, dass Systemadministratoren Rohdaten oder Datenbankinhalte nicht lesen dürfen, muss bei der Verarbeitungs-Software entsprechende Mechanismen implementieren. So werden Daten vor dem Schreiben verschlüsselt und beim Lesen entschlüsselt.

Wer auf Nummer sicher gehen will, legt ebenfalls fest, wie die Daten auf den Diskspeichersystemen zu liegen haben. Es empfiehlt sich, Daten auf pro Anwendung dedizierten Disks zu speichern. Dies hat den Vorteil, dass für Performance und Sicherheit der Daten spezifische Massnahmen ergriffen werden können. Dedizierte Datendisks ermöglichen zudem eine zusätzliche Verschlüsselung. Sollten sie in falsche Hände geraten, können daraus keine Daten extrahiert werden.

Sicherheitsmassnahmen können jedoch auch zu Abstrichen bei der Verfügbarkeit führen, wenn kein durchdachtes Schlüsselmanagement besteht. Der Zugriff auf den Schlüssel muss auf möglichst wenige Personen beschränkt sein. Liegt dieser beispielsweise beim Kunden, so muss auch der Hoster morgens um 3 Uhr darauf zugreifen können, um beispielsweise ein System neu zu starten. Natürlich gibt es dafür technische Lösungen. Schlüsselsysteme bringen aber weitere Abhängigkeiten mit sich, welche die Verfügbarkeit gefährden können.

BACKUP & RESTORE

Daten müssen auch als Backup gesichert werden, also in einer vom primären Standort der Daten getrennten Lokalität und auf einem vom primären Datenträger getrennten Medium. Auch hier kommen die bereits beschriebenen Techniken zur sicheren Übertragung zum Einsatz. Die Daten werden idealerweise vor der Übertragung auf das Backup-Medium des Quellsystems verschlüsselt. Auf dem Sicherungsmedium befinden sich somit unlesbare Daten, bzw. Daten, die nur mit dem auf dem Quellsystem bekannten Schlüssel gelesen werden können. Die Verfügbarkeit ist im Fall einer Disaster Recovery oder Business Continuity aber auch in diesem Fall nur gegeben, wenn der Kunde über den entsprechenden Schlüssel verfügt und die typengleiche Backup-Restore-Software benutzt.

«Alle Daten mit denselben Auflagen zu versehen, führt zu hohen Kosten und Abhängigkeiten»

Kaspar Geiser

DAS LÖSCHEN VON DATEN

In Zeiten der Cloud ist das Löschen von Daten kaum mehr möglich. Natürlich ist oft vom «Recht auf Vergessenwerden» die Rede, das Google dazu brachte, auf Geheiss gewisse Daten nicht mehr anzuzeigen. Die Daten selber werden dabei aber nicht gelöscht, sie erscheinen einfach nicht mehr in den Suchresultaten. Auch für einen Hoster gibt es nicht das eine Löschen. Werden Daten auf dem primären System gelöscht, stehen diese mindestens während der definierten Backup-Aufbewahrungszeit für die Wiederherstellung bereit. Das heisst, die Löschung auf den Backup-Medien geschieht mit einer entsprechenden Verzögerung. Stellt jedoch ein Projekt die Anforderung, dass nach Einstellung des Betriebs sämtliche Daten beim Hoster komplett gelöscht sein müssen, impliziert dies technische Massnahmen. Eine davon sind pro Kunde dedizierte Medien. Nur dann können die Daten definitiv vernichtet werden, technisch und je nach Sicherheitsstufe auch mechanisch: im Schredder.

KLARE VORSTELLUNG, KLARE VORGABEN

Wenn in einem Projekt sensitive Daten entstehen oder verarbeitet werden, müssen die Anforderungen an sie explizit formuliert werden. Erst aus einer solchen Definition lassen sich technische Implementierungen ableiten, welche die Daten entsprechend schützen. Alle Daten mit denselben Auflagen zu versehen, führt zu hohen Kosten und Abhängigkeiten von Dienstleistungsanbietern. Die Verschlüsselung von Daten beim Hoster ist eine sinnvolle Möglichkeit, den Zugriff einzuschränken. Wichtiger ist aber die klare Vorstellung oder Vorgabe, wo die Daten effektiv lagern, wer Zugriff zu diesen hat und mit welchen Massnahmen diese vor Veränderung geschützt werden. Dies wiederum bedingt eine uneingeschränkte Transparenz des Hosting-Anbieters in Technik und Prozesse. ←

Kaspar Geiser ist Geschäftsleiter des Hosting-Anbieters Aspectra AG → **www.aspectra.ch**