DAS BACK-UP-TRIUMVIRAT

Back-up und Disaster Recovery müssen über eine reine Sicherung von Daten hinaus aktuell einiges leisten. Vor allem die einfache und zuverlässige permanente Sicherung und anwendungskonsistente Wiederherstellung von Informationen. Eine zeitgemäße Lösung zahlt sich aber auch bei IT-Sicherheit und im Datenschutz aus.

Autor: Sven Haubold **Redaktion: Axel Pomper**

➤ Eine in diesem Frühjahr von Arcserve durchgeführte Umfrage unter 600 Kunden und Partnern weltweit hat aufgezeigt, dass für Unternehmen vor allem die Flexibilität und Einfachheit der Sicherung und der Wiederherstellung von Daten von entscheidender Bedeutung sind. Die fast schon sprichwörtliche Klage über den Mangel an Ressourcen spielt dagegen offenbar keine so große Rolle. Laut der Studie fürchten viele der befragten Entscheider die Kosten einer Downtime, die Komplexität und den Aufwand einer Sicherung oder eine Ransomware-Verschlüsselungsattacke mehr als mangelnde Ressourcen.

Einfachheit

In der Verwaltung heterogener Datensysteme sehen viele der Befragten mittlerweile die größte Herausforderung, um Daten und Anwendungen zuverlässig zu sichern. 45 Prozent der Anwender gaben an, dass für sie eine einfache Einrichtung und Verwaltung die Hauptkaufargumente für den Erwerb einer Sicherungslösung sind – noch vor deren Gesamtkosten. Unternehmen sind offensichtlich bereit, mehr für eine einfache Lösung zu zahlen, anstatt ein preisgünstigeres, aber schwerer zu handhabendes Angebot, das mehr Training, Spezialisierung und letzten Endes auch Zeit erfordert, zu wählen.

Die meisten Anwender verlangen daher nach einer einfachen Sicherung und Wiederherstellung mit zentralem Management sowie Lösungendas, die flexibel virtuelle, physische, Cloud- und On-Premise-Sicherungen unterstützen. Auch die Wiederherstellung virtueller Maschinen oder ein Bare Metal Recovery sollte schnell möglich sein.

Hochverfügbarkeit

Eine schnelle Wiederverfügbarkeit prinzipiell aller Daten in Produktivsystemen ist letztlich das K.O.-Kriterium. Die Befragten der Umfrage halten dementsprechend 79 Prozent ihrer Daten für unternehmenskritisch. Die gestiegenen Ansprüche der 24/7-Wirtschaft erlauben immer geringere Verluste bei Einspielung einer Sicherung. Daten müssen so aktuell wie möglich aus kontinuierlichen Replikationen von aktuellen Beständen wiederhergestellt werden. Zugleich müssen sich aus einer Sicherung Informationen anwendungskonsistent abrufen lassen, sodass das Programm umgehend mit den entsprechenden Datensätzen weiterarbeiten kann – etwa mit einer E-Mail, die direkt wieder in die Mailbox des entsprechenden Mitarbeiters erstellt wird.

Hochverfügbarkeitslösungen synchronisieren daher kontinuierlich die Daten auf Produktionsservern mit einem zweiten Replika-Server (physisch oder virtuell), der lokal, an einem beliebigen Remotestandort oder in der Cloud bereitgestellt wird. Im Desaster-Fall – ob durch einen Hardwareausfall, einen böswilligen Angriff, höhere Gewalt, einen Stromausfall oder eine misslungene Softwareinstallation – muss der Failover, also die Umleitung der Endnutzer auf den Replikationsserver, unmittelbar und automatisch erfolgen, um den Geschäftsbetrieb aufrechtzuerhalten. Das gilt auch für den Failback, wenn der Produktionsserver wieder zur Verfügung steht.

Für eine angemessene Aktualität der wiederhergestellten Daten sorgt ein zeitgemäßes Back-up mit Echtzeitreplikationen, um auch Wiederherstellungspunkte, die wenige Minuten zurückliegen, mit Sekundengenauigkeit anzusteuern. So lässt sich etwa der Datenstatus unmittelbar vor dem Start einer Ransomware-Attacke sichern. Wie bei einem Audiomedium kann die IT auf einen beliebigen Datenstand

zurückspulen – etwa drei Minuten und zwölf Sekunden, bevor eine Verschlüsselungsattacke begann.

Speicherunabhängige Lösungen können Daten sichern, egal welche Art von Sicherungsmedien in den Produktivumgebungen verwendet wird – DAS, NAS oder SAN. Bei Netzen mit eingeschränkter Bandbreite und hoher Latenz bieten entsprechende Lösungen WAN-Optimierungsfunktionen mit Komprimierung, Bandbreitendrosselung, Multi-Stream-Replikation, periodischer Replikation oder Offline-Synchronisierungsoptionen zur Anpassung an die Leistungsfähigkeit des Netzes. Nicht zu vergessen ist auch die permanente automatisierte Überprüfung der Sicherung auf ihre Funktionsfähigkeit.

Bildc. Le Moal Olivier - i123rf

Back-up und Disaster Recovery sollen in Teilen ebenso die Datensicherheit unterstützen. Eine solche Hilfe ist angesichts der Datenschutz-Grundverordnung nicht unwichtig. Die DSGVO gibt jedem EU-Bürger das Recht, seine Einwilligung in die Erhebung persönlicher Daten zurückzuziehen. Das schließt auch die endgültige Löschung seiner E-Mails und anderer personenbezogener Informationen mit ein.

Datenschutz

E-Mail-Archivierungslösungen können in vielen Fällen über die Sicherung hinaus eine Möglichkeit zur gezielten Informationssuche für die Weitergabe von Daten zur Löschung oder zur Wiederherstellung bieten. Filtering-Funktionen sollen es ermöglichen, Anfragen von Kunden nach über sie gespeicherte Daten sowie nach deren Verarbeitung, Weitergabe und Löschung zu beantworten und dabei berechtigte Unternehmensinteressen berücksichtigen. So haben die Verantwortlichen etwa die Möglichkeit, Daten eines Kunden etwa bei einem noch laufenden Verfahren im Back-up zu sichern, auch wenn der Kunde eigentlich die Löschung beantragt oder durch Kündigung die Erlaubnis der Speicherung implizit widerrufen hat. Diese Daten dürfen gesichert, aber nicht mehr in Produktivanwendungen wiederhergestellt werden. Das Unternehmen muss sie entsprechend bei der Sicherung kennzeichnen.

E-Mail-Archivierungslösungen stellen zudem Funktionalitäten zur Verfügung, um die Konformität der Unternehmens-IT mit den Anforderungen etwa der DSGVO effektiv zu unterstützen. Dazu gehören die verschlüsselte Datensicherung und die Wiederherstellung aus einer einheitlichen Konsole, die granulare Wiederherstellbarkeit von Datensätzen mit der Möglichkeit, spezifische Daten auszuschließen oder unterschiedlich zu behandeln. So können Mails nach Standort, Bereich oder Abteilung gefiltert werden.

Eine Verschlüsselung der E-Mails bei der Sicherung unterstützt bei richtiger Implementierung auch die DSGVO-Forderung nach „privacy by design“. Ein Reporting aller Aktivitäten über Ort und Zeit der Sicherung sowie Retention Reports, die belegen, wie lange Kopien der Datensicherung aufbewahrt und wann sie zerstört werden, können die Unternehmen bei Erfüllung der Vorgaben der DSGVO zur Dokumentation der Einhaltung von Datenschutzbestimmungen unterstützen. In keinem Fall darf aber die notwendige Hinzuziehung professioneller rechtlicher Beratung und die Bestellung eines internen oder externen Datenschutzbeauftragten unterbleiben.

Sven Haubold ist Territory Account Director bei Arcserve