Quelle: Attingo

Datenrettung durch externe Dienstleister

Professionelle Hilfe beim Speicher-Crash

von Nicolas Ehrschwendner

IT-Verantwortliche in Unternehmen lösen technische Probleme am laufenden Band. Sie sind überall zur Stelle, wo es brennt. Doch es gibt auch Situationen, in denen sie machtlos sind. Wenn beispielsweise Defekte in den Speichersystemen eines Unternehmens auftreten, wird es ernst. Können die Mitarbeiter nicht mehr auf die Daten zugreifen oder es gehen Daten komplett verloren, stoßen auch viele Administratoren an ihre Grenzen. IT-Administrator zeigt in diesem Artikel einerseits Tücken von Speichersystemen auf. Andererseits erfahren Sie, worauf Sie achten sollten, wenn Sie sich Hilfe durch professionelle Datenretter holen.

Die meisten Unternehmen versuchen, einem Verlust von Daten bestmöglich durch moderne Speicher-Management-Systeme vorzubeugen. Damit im Ernstfall die dort gespeicherten Unternehmensdaten wiederhergestellt werden können, beinhalten solche Systeme automatische Backup-Funktionen. Zum Beispiel bietet sich hier die Speichertechnik CDP (Continuous Data Protection) an. Diese erfasst Änderungen kontinuierlich, anstatt punktuelle Backups anzulegen, die dann viel Zeit und Speicherplatz beanspruchen. Ganz gleich, welche Speichertechnik zum Einsatz kommt, Administratoren können mithilfe der regelmäßig angelegten Sicherungskopien zwar bei vorübergehenden Speicherproblemen und kleineren Fehlern Datenverlust verhindern. Bei gravierenden Schäden am Speichermedium selbst müssen jedoch in der Regel Experten herangezogen werden, um die Unternehmensdaten zu retten.

NAS und seine Tücken

Viele Firmen setzen zur Sicherung ihrer Daten auf Network Attached Storage (NAS). Dies sind Speichermedien, die ähnlich wie ein Computer aufgebaut sind. Sie sind beliebt, weil sie flexibel an vielen Arbeitsplätzen einsetzbar sind, ganz unabhängig vom Betriebssystem. Jedoch treten immer wieder Probleme beim Zugriff auf NAS-Daten auf. Ursachen dafür können Festplattenausfälle sein, Bedienungsfehler, aber auch Bugs in der NAS-Software. Häufig verursachen aber auch Updates der Firmware Probleme, also Aktualisierungen der Hardware-nahen Basis-Software, ohne die das NAS nicht funktioniert. Bei solchen Updates wird oft der logische Aufbau der Dateiablage unabsichtlich verändert, so dass das NAS keinen Zugriff mehr auf die gespeicherten Daten hat. Deshalb empfiehlt es sich, vor einem Update der NAS-Firmware Sicherungskopien anzulegen. Dies ist zwar nicht immer ganz einfach, schützt aber möglicherweise vor Datenverlust. Denn um Daten in einem NAS retten zu können, auf die der Administrator keinen Zugriff mehr hat, müssten alternativ externe Dienstleister beauftragt werden, die sich auf Notfälle spezialisiert haben.

Datenverlust in RAID-Systemen

Innerhalb eines NAS fällt oft die Wahl auf ein RAID-System. RAID steht für "Redundant Array of Independent Disks", also einen Speicherverbund aus mehreren einzelnen Festplatten. Mit einem RAID lässt sich eine besonders hohe Speicherkapazität bei relativ überschaubaren Kosten erreichen. Bei den meisten RAID-Systemen werden die Daten mit redundanten Informationen im Datenträgerverbund abgespeichert.

Eine Ausnahme stellt hier lediglich das RAID 0-System dar, das aus einem Verbund von unabhängigen Festplatten besteht, die zu einem Speichermedium zusammengeschlossen werden. RAID 0 ermöglicht zwar einen schnellen Zugriff auf alle Platten gleichzeitig, birgt aber auch das Risiko des Datenverlustes, wenn nur eine einzelne der Festplatten ausfällt. Andere RAID-Systeme sorgen durch das Speichern redundanter Daten dagegen dafür, dass trotz Ausfalls einer oder mehrerer einzelner Festplatten im Datenspeicher alle Daten verfügbar bleiben.

Aufgrund der relativ geringen Kosten ist beispielsweise das RAID 5-System weit verbreitet. Dafür benötigt der Nutzer mindestens drei Festplatten. Bei RAID 5 werden entsprechend dem Algorithmus des RAID-Controllers die Parity-Daten auf den angeschlossenen Festplatten verteilt. Über diese Parity-Daten lassen sich verlorene Daten wiederherstellen, auch wenn auf eine der Festplatten im Verbund gar nicht mehr zugegriffen werden kann.

Bei dem weniger verbreiteten RAID 4 dagegen werden die Parity-Daten nicht verteilt, sondern nur auf einer Festplatte gespeichert. Ein Nachteil von RAID 5 ist allerdings die relativ geringe Schreibgeschwindigkeit. Das Verfahren eignet sich daher am besten für große Datenmengen, die sich auf viele kleine Dateien verteilen.

RAID 6 bietet im Vergleich zu RAID 5 noch etwas mehr Sicherheit, da es sogar bei einem Ausfall von zwei Festplatten noch funktioniert. RAID 6 wird im Handel unter anderem auch unter dem Namen "Advanced Data Guarding" angeboten und umfasst mindestens vier Festplatten. Doch auch bei RAID 6-Systemen droht endgültig Datenverlust, wenn mehr als zwei Festplatten im Speicherverbund beschädigt sind.

Rebuild birgt besonderes Risiko

Festplatten können zum Beispiel durch einen Head-Crash irreparabel beschädigt werden. Dabei berührt der Lese- und Schreibkopf direkt die Festplattenoberfläche, was etwa durch Erschütterungen oder falschen Einbau der Festplatte geschehen kann. Ebenso kann Überspannung, zum Beispiel durch einen Blitzschlag, Defekte verursachen. In solchen Fällen kann der Administrator versuchen, die Daten auf der beschädigten Festplatte innerhalb des RAID-Systems wiederherzustellen.

Doch gerade im Prozess der Datenwiederherstellung aus den Parity-Daten, dem sogenannten Rebuild, kann es zu Komplikationen kommen. Denn für das Rebuild muss der RAID-Controller auf alle Festplatten zugreifen und die dort noch vorhandenen Daten auslesen. Fällt während dieses Vorgangs eine weitere Festplatte aus oder findet der Controller neue beschädigte Sektoren, ist auf das gesamte RAID-System kein Zugriff mehr möglich. Der Wiederherstellungsvorgang bricht ab.

Ein häufiges Problem bei RAID-Systemen in Windows-Servern ist der Einsatz des Windows-Prüfprogramms Checkdisk (CHKDSK) beziehungsweise Scandisk. Während das Hilfstool an anderer Stelle zuverlässig Dateisystemfehler reparieren kann, führt es beim Einsatz in RAID-Systemen zu Defekten, indem es die innere Logik des RAID-Systems zerstört. Innerhalb einer RAID-Anordnung sollte man das Programm deshalb in der Windows-Registry deaktivieren, um einen automatischen Start von Checkdisk auszuschließen.

SSD-Speicher schützen nicht vor Datenverlust

Als Speichermedium der Zukunft gelten derzeit Solid State Drives, kurz SSD. Wie der Name verrät, liegt deren großer Vorteil in ihrer Robustheit. Denn SSDs sind, anders als Festplatten, nicht aus vielen kleinen mechanischen Einzelteilen aufgebaut. Sie enthalten beispielsweise keine Lese- und Schreibköpfe und keine Magnetscheiben. Das oben beschriebene Head-Crash-Szenario ist hiermit ausgeschlossen. Stattdessen bestehen sie aus Flashspeicher-Bausteinen. So arbeiten sie im Vergleich zu Festplatten lautlos und verbrauchen weniger Strom. Auch die Geschwindigkeit beim Start von Windows oder dem Zugriff auf Datenbanken ist höher. Doch trotz des völlig anderen Aufbaus von SSD ist die Sicherheit nur trügerisch. Gerade die scheinbare Robustheit der Datenträger kann zu unsachgemäßer Handhabung und zu physikalischen Schäden führen.

SSDs sind im Allgemeinen schockresistenter als gewöhnliche Festplatten. Durch einen Sturz können aber trotzdem beispielsweise Haarrisse auf der Platine oder auch Beschädigungen der Kontakte entstehen. Äußere Einflüsse wie Wasser können Defekte hervorrufen, etwa einen Kurzschluss. Ebenso können Fehler in der Firmware bei SSDs zu Datenverlust führen, aber auch zu logischen Problemen, zum Beispiel wenn der Datenträger während eines laufenden Datentransfers von der Schnittstelle abgezogen wurde. Insgesamt haben SSDs also im alltäglichen Gebrauch viele Vorteile, schützen aber keinesfalls vor dem Verlust von Daten. Auch hier empfiehlt es sich, regelmäßige Backups anzulegen, wie bei jedem Speichermedium.

Im Ernstfall Experten konsultieren

Je nachdem, welche Daten durch IT-Fehler verloren gehen, drohen dem betroffenen Unternehmen hohe wirtschaftliche Schäden, Imageverlust, rechtliche Konsequenzen oder im schlimmsten Fall der Konkurs. Beispielsweise gibt es für bestimmte Unternehmensdaten Aufbewahrungspflichten, weshalb auch der Zugriff auf archivierte Daten immer gewährleistet sein muss. Deshalb ist es entscheidend für ein Unternehmen, dass bei Problemen mit den Speichermedien die richtigen Entscheidungen getroffen werden. Zwar gibt es eine Reihe von Software-Tools, die Hilfe im Notfall versprechen. Jedoch stoßen diese bei Hardware-Schäden schnell an ihre Grenzen.

Wer sich an die Hardware selbst heranwagt und Festplatten öffnet, muss sich bewusst sein, dass die Technik äußerst empfindlich ist. Schon ein scheinbar einfacher Eingriff in die Hardware birgt ein hohes Risiko und kann zum Totalausfall führen. Dies erhöht zusätzlich den Aufwand für professionelle Datenretter. Eine risikoarme Reparatur sollte deshalb in einem Reinraumlabor stattfinden.

IT-Administratoren sollten im Ernstfall auf Experten für Datenrettung vertrauen, sonst laufen sie Gefahr, durch gescheiterte Rettungsversuche Zeit zu verlieren und den Schaden nur zu vergrößern. Die Wahrscheinlichkeit, die Daten dann im Nachhinein noch retten zu können, wird immer geringer. Fachleute können den Schaden auf schnelle und diskrete Weise in Grenzen halten.

Doch woran erkennen Sie seriöse, zuverlässige Anbieter? Schließlich verlassen Sie sich nicht nur darauf, dass sie die Rettung in technischen Notfällen darstellen. Sie vertrauen ihnen auch Unternehmensdaten an, die normalerweise niemand von außen einsehen kann und darf. Hinzu kommt das Phänomen, das manche Privatleute vielleicht auch von Schlüsseldiensten kennen: So manche "Retter" nutzen die schwierige Lage ihrer Kunden durch überhöhte Preise aus, welche die Kunden nur aufgrund ihrer ausweglos erscheinenden Lage zu zahlen bereit sind.

Seriöse Datenretter

Wichtig sind in der Kommunikation zwischen Kunde und Dienstleister vor allem Vertrauen und Transparenz. Der Anbieter muss seinem Kunden deutlich machen, welche technischen Möglichkeiten er in seiner Situation hat und ihn kompetent beraten, damit die richtigen Entscheidungen getroffen werden können. Dazu gehört als erster Schritt unbedingt eine Analyse des Status Quo, die anschließend mit dem Geschäftsführer oder IT-Verantwortlichen besprochen wird. Auf dieser Grundlage kann der Kunde entscheiden, ob überhaupt eine professionelle Datenrettung durchgeführt werden soll. So behält das Unternehmen einen Überblick über die anfallenden Kosten für den Notfall-Einsatz. Im Voraus einen Pauschalpreis zu versprechen, ist dagegen unseriös. Auch wenn die Kosten sich im Rahmen einer gewissen Preisspanne bewegen sollten, sind sie in der Regel nicht exakt vorhersehbar. Zudem sollten laut Attingo-Datenrettungsexperte und Mitgeschäftsführer Peter Franck Datenretter unter anderem eine spezielle Ausstattung und ein großes Kontingent an Ersatzteilen mitbringen.

Im Vorfeld recherchieren

Auch wenn es im Notfall schnell gehen muss, sollten Sie im Vorfeld versuchen, sich ein Bild von dem Dienstleister zu verschaffen. Empfehlungen finden Sie zum Beispiel über spezielle Internetforen, wo sich Erfahrungen mit anderen Administratoren austauschen lassen. Datenschutz ist für externe, seriöse Dienstleister dabei oberstes Gebot. Weder dürfen Unternehmensdaten in die Hände Dritter weitergegeben werden noch Informationen über den Datenrettungsprozess an sich. IT-Verantwortliche sollten deshalb dem Anbieter gezielt Fragen stellen, bevor sie einen Auftrag erteilen, etwa: Wo genau und von wem werden die Daten eingesehen, bearbeitet oder gespeichert? Bei einem sensiblen und heiklen Thema wie Datenrettung kommt es nämlich darauf an, trotz einer prekären Lage besonnen zu handeln und zuvor alle Optionen abzuwägen. *(dr)*

Nicolas Ehrschwendner ist Geschäftsführer bei der Attingo Datenrettung GmbH.