

Bei Datenverlust können professionelle Datenretter Krankenhäusern wertvolle Unterstützung leisten

Beim Daten-Doktor in Behandlung

Datenverlust ist das Schreckgespenst jedes IT-Administrators. Sind plötzlich sämtliche Patienten- oder Abrechnungsdaten für die Krankenkassen verschwunden, ist die Gefahr von Panikreaktionen groß. Neben wirtschaftlichen Schäden und Imageverlust drohen auch juristische Konsequenzen, da Krankenhäuser verpflichtet sind, bestimmte Daten aufzubewahren. Ganz zu schweigen von Problemen bei der Patientenversorgung, wenn komplette OP-Pläne, dringend benötigte Voruntersuchungen oder Medikationspläne verschwunden sind. Deshalb müssen Administratoren bei technischen Problemen besonnen vorgehen und ‚Schnellschüsse‘ vermeiden.

IT-Verantwortliche in Krankenhäusern versuchen, einem Datenverlust bestmöglich durch moderne Speicher-Managementsysteme vorzubeugen, die automatische Backup-Funktionen beinhalten. Bei schweren Schäden an den Datenträgern selbst müssen jedoch in der Regel Experten herangezogen werden, um die Daten zu rekonstruieren.

Die Zeit ist bei der Datenrettung ein wichtiger Faktor

In vielen Fällen spielt neben der Datenrekonstruktion auch der Zeitfaktor eine große Rolle, wie schnell die geretteten Daten wieder zur

Verfügung stehen – in der Fachsprache als Recovery Time Objective (RTO) bezeichnet. Jeder Tag, an dem nicht abgerechnet werden kann, kommt dem Krankenhaus teuer zu stehen. Jeder Tag, an dem Patienten aufgrund fehlender Informationen nur unzureichend behandelt werden können, verursacht Kosten und Unmut.

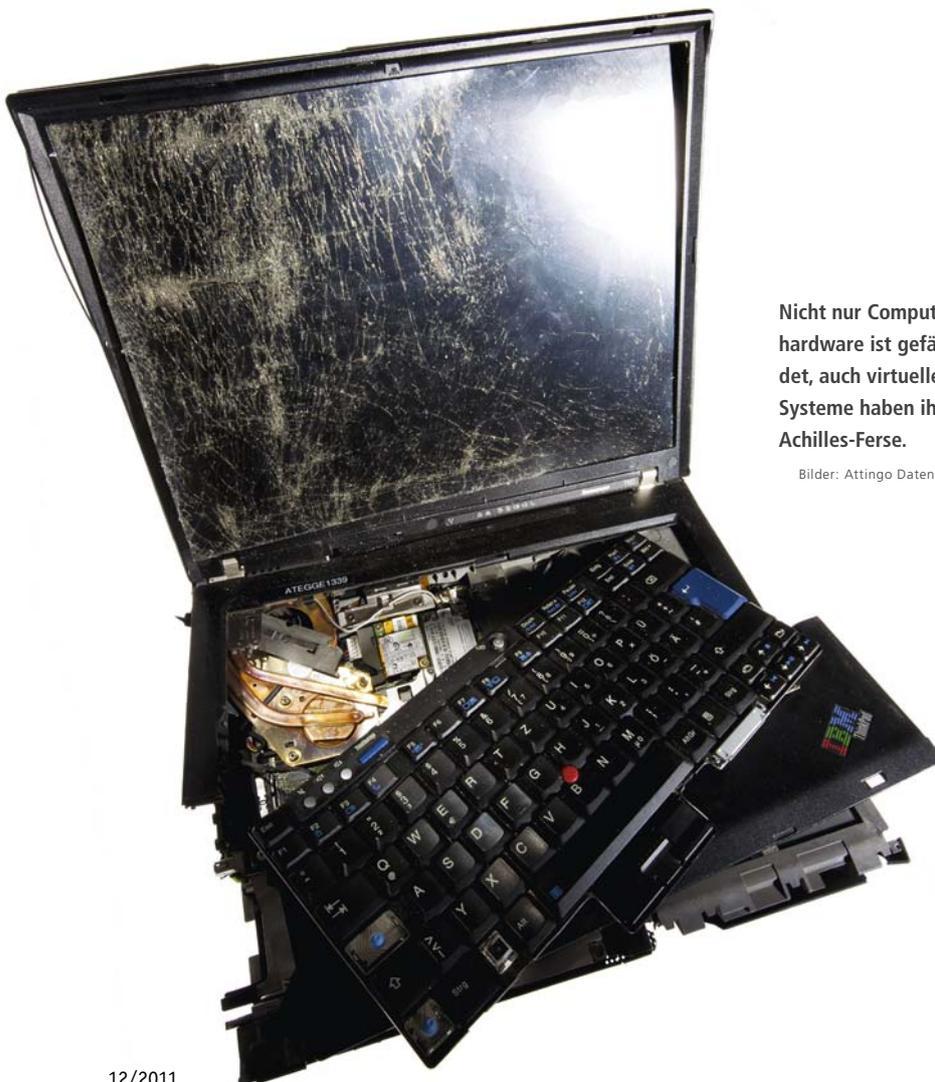
Datenverlust ist nicht gleich Datenverlust, sondern kann in unterschiedlichen Facetten auftreten. Spezialisten wie die Attingo Datenrettung GmbH bieten dafür entsprechende Lösungen an.

Auch in einem Raid-System (Redundant Array of Independent Disks), also einem Verbund mehrerer Speichermedien, können schwere Defekte auftreten. Das Ziel dieser Raid ist vor allem, die Ausfallsicherheit und Leistungsfähigkeit durch mehrere Festplatten zu erhöhen.

Raid-Systeme bieten im Allgemeinen den großen Vorteil relativ geringer Kosten bei gleichzeitig hoher Speicherkapazität. Mit Ausnahme von Raid 0 werden die Daten redundant auf mehreren Festplatten gespeichert. Am häufigsten sind die Raid-Level 1, 5, 6 und 10 verbreitet. Raid 1, auch Mirroring genannt, bietet eine hohe Sicherheit, da die Daten gespiegelt werden. Es kommt deshalb nicht selten in Krankenhäusern zum Einsatz, insbesondere als externes NAS-System (Network Attached Storage), wie es inzwischen viele Hersteller anbieten. Dabei werden meist zwei Festplatten verwendet, wobei sämtliche Schreibzugriffe parallel auf einem zweiten Datenträger erfolgen. Fällt ein Datenträger aus, sind die identischen Informationen auf dem zweiten gespeichert. So die Theorie. Die Praxis zeigt jedoch, dass eine Festplatte durch Fehlfunktionen des Controllers oder auch falsche Konfiguration ausfallen kann, ohne dass eine Fehlermeldung an den Administrator weitergeleitet wird. Das System läuft dann nur noch mit einer Festplatte weiter, eine Spiegelung der Daten findet nicht mehr statt. Fällt im Laufe der Zeit die zweite aus, ist keine redundante Festplatte mehr verfügbar. Weiterer Nachteil von Raid 1 ist, dass durch die Spiegelung nur die Hälfte der Speicherkapazität für die Datenspeicherung genutzt werden kann.

Nicht nur Computerhardware ist gefährdet, auch virtuelle Systeme haben ihre Achilles-Ferse.

Bilder: Attingo Datenrettung





Wichtig für den Daten-Doktor ist, dass er die genauen Umstände des Datenverlusts, des Crashes und der vorhandenen Performance kennt, um möglichst viele Informationen retten zu können.

Raid 5 für die gleichmäßige Festplattenbeanspruchung

Sehr beliebt ist der Einsatz von Raid-5-Verbunden. Sie bieten im Vergleich zu Raid 1 eine höhere Leistungsfähigkeit und sind dabei vergleichsweise kostengünstig. Durch die blockweise Speicherung der Nutzdaten auf dem gesamten Raid-Verbund erfolgt eine gleichmäßige Verteilung der Daten auf die Festplatten. Dies hat zur Folge, dass die Parity-Daten blockweise wechseln und alle Festplatten gleichmäßig beansprucht werden. Folglich sind beim Ausfall eines Datenträgers alle Informationen auf den übrigen Festplatten vorhanden. Für den Rebuild-Vorgang, also den Wiederherstellungsprozess vom Degraded- in den Normalzustand, werden vom Raid-Controller so genannte Parity-Daten beansprucht. Durch einen Defekt auf einer einzelnen Festplatte ist der Rebuild-Vorgang also nicht unmittelbar gefährdet. Doch er birgt Risiken: In dieser Zeit muss der Raid-Controller die Rohdaten aus allen vorhandenen Festplatten auslesen. Treten währenddessen neue Defekte auf – dies können einfache Lesefehler sein oder ein Ausfall durch Überspannung –

bricht in den meisten Fällen der Vorgang unvollständig ab. Folglich ist kein Zugriff auf den Verbund mehr möglich.

Je höher die Plattenanzahl und je älter das System ist, desto höher ist das Risiko solcher Ausfälle. Wie bei Raid-1-Verbunden besteht auch bei einem Raid-5-System die Gefahr, dass bereits schon vorher ein Datenträger ausgefallen ist und keine Fehlermeldung ausgeworfen wurde. Das System lief im Degraded-Mode, ohne dass dies dem Administrator protokolliert wurde.

Um die Sicherheit zu erhöhen, setzen IT-Administratoren in Krankenhäusern verstärkt auf Raid-6-Verbunde, die im Vergleich zu Raid 5 den Vorteil bieten, dass sie den Ausfall von zwei Festplatten verkraften. Je nach IT-Landschaft wird heutzutage vermehrt auf SAN (Storage Area Network) zurückgegriffen. Oft als Mehrplattensystem im Raid-Verbund verbaut, erfreut es sich großer Beliebtheit, da es an einen Server angeschlossen, flexibel für verschiedene Einsatzzwecke aufgeteilt werden kann. Doch auch bei SAN-Systemen können Probleme beim Zugriff auf die Daten auftreten. Neben den beschriebenen Festplattenausfällen und Bedienungsfehlern können auch Bugs oder Firmwarefehler Ursache für einen

Datenverlust sein. Vor dem Aufspielen von Updates empfiehlt es sich, Sicherungskopien der Daten anzufertigen. Oft scheitert dies aber an der Zeit und den Kosten, da das Anlegen solcher Kopien je nach Kapazität mehrere Stunden in Anspruch nehmen kann.

Risiken und Gefahrenquellen lauern überall

Zudem muss entsprechende Hardware verfügbar sein, die sofort zum Einsatz kommen kann, wenn es zu Problemen beim Aufspielen der Updates kommt. In Anbetracht klammer Kassen bei den Krankenhäusern wird meist auf diese Schritte verzichtet. Attingo-Geschäftsführer Nicolas Ehrschwendner sieht die Zwickmühle, in der sich die IT-Administratoren befinden: „In vielen Fällen klappt es ja auch. Problematisch wird es, wenn es mal nicht funktioniert und ein Zugriff aufs System nicht mehr möglich ist. Dann ist der entstandene Schaden ganz schnell sehr groß.“

Ein ebenfalls häufiges und fatales Szenario ist der Ausfall des Raid-Controllers, sei es im NAS oder im Server. So kann es vorkommen, dass trotz Tausch des Raid-Controllers ein Zugriff auf den Raid-Verbund nicht mehr möglich ist, da controllerspezifische Parameter auf den Festplatten gespeichert sind. Dies ist deshalb besonders ärgerlich, da eine Datenrettung notwendig ist, obwohl keine Festplatte defekt ist. Hinzu kommt, dass diese Problematik nicht allein bei Raid 1, sondern auch bei Raid 5 und 6 auftreten kann.

Eine weitere Gefahrenquelle können von außen verursachte Fehler sein. So schützen Raid-Verbunde nicht vor Hacking-Angriffen, manuellem Löschen, Datenbankproblemen oder Software-Bugs.

Auch virtuelle Umgebungen sind betroffen

In Krankenhäusern werden virtuelle Umgebungen gerade in Sparzeiten immer beliebter. Wer nicht mehrere Server nebeneinander aufstellen, betreiben und warten will, greift gerne zu Virtualisierungstechnolo-

gien, die alles auf einer einzigen starken Maschine bündeln. Gerade die Administration virtueller Systeme bietet erhebliches Einsparungspotenzial. Ein weiterer Vorteil ist die bessere Auslastung der Server. Durch die Bündelung verringert es zudem die Anschaffungskosten, da lediglich Speicherkapazität in Form weiterer Festplatten erweitert werden muss und die vorhandene Hardware genutzt werden kann. Doch Datenretter schlagen Alarm und warnen vor den Schattenseiten dieser Technologie. Insbesondere bei virtuellen Servern können kleine Fehler oft große Auswirkungen haben. Ein unbedachtes Löschen einer Datei in Form eines ganzen virtualisierten Servers kann dazu führen, dass sämtliche Daten verloren sind – je nach Hostsystem mit einem Mausklick, ohne Kontrollfenster. Bedienungsfehler sind bei virtuellen Systemen keine Seltenheit und haben entsprechend schwerwiegende Folgen.

Daneben besteht aber eine weitaus größere Gefahr: Die Bündelung der Daten auf nur sehr wenige ‚echte‘ Server hat zur Folge, dass bei einem Ausfall sämtliche virtuelle Server betroffen sind. Doch gerade aus Gründen eingeschränkter Budgets wird teilweise auf redundante Server verzichtet. Zudem muss bei redundanten Servern neben hohen Anschaffungskosten auch die Administration des Datentransfers großer Datenmengen berücksichtigt werden.

Die Einsätze der Datenretter häufen sich

In letzter Zeit häufen sich die Fälle, in denen Datenretter bei Ausfällen virtueller Systeme gerufen werden. Eine Datenrettung ist auch hier möglich, in einigen Fällen jedoch komplexer. Der Grund: Sowohl das virtuelle Betriebssystem als auch das Dateisystem sind in der Regel pro-



Selbst Daten auf Raid-Systemen sind nicht vor Verlust geschützt. Häufig kommt es vor, dass Festplatten Fehler aufweisen, ohne dass der Administrator eine Fehlermeldung erhält.

prietär, das heißt, geistiges Eigentum des Herstellers und daher auch nicht öffentlich dokumentiert. Nur sehr wenige Datenrettungsunternehmen verfügen über das entsprechende Know-how.

Nicolas Ehrschwendner beschreibt den Sachverhalt folgendermaßen: „Wir betreiben laufend zeit- und kostenintensives Reverse-Engineering, um Kunden im Ernstfall schnell



Monatlich fundierte Informationen über praxisorientierte Problemlösungen für Entscheider im Krankenhaus machen Sie zum gut informierten Gesprächspartner.

Nur ein Abonnement sichert Ihnen eine regelmäßige Lieferung.

Jetzt abonnieren!

Bitte an +49 (0) 88 06-95 77-11
faxen oder einsenden an:

pnverlag Dr. Wolf Zimmermann
Vertrieb/Abo-Service
Leitenberg 5
D-86923 Finning

ktm@pn-verlag.de
www.ktm-journal.de

Ja, bitte senden Sie mir ab sofort monatlich KTM zum Komplettpreis
Inland: Euro 82,00 (Ausland: Euro 92,00)

Name, Vorname

Funktion

Firma/Krankenhaus

Straße/Postfach

PLZ, Ort

Tel./Fax

E-Mail

helfen zu können. Nur mit tiefgreifendem Wissen über interne Systemstrukturen (zum Beispiel Firmware), Algorithmen (zum Beispiel Verlauf der Parity) und Verhaltensweisen von Raid-Controllern ist eine schnelle und zuverlässige Rekonstruktion von Raid-Systemen machbar. Unsere Techniker haben Verfahren entwickelt, um Raid-Systeme fast aller Hersteller per Software zu simulieren. Raid-Systeme können auch dann rekonstruiert werden, wenn fatale Rebuilds mit falschen Datenträgern oder falscher Reihenfolge gestartet oder Raid-Konfigurationen gelöscht und neu angelegt wurden. Das Know-how in virtualisierten Umgebungen über Host-Betriebssysteme und logische Volume Manager, Host-Dateisysteme, Gast-Betriebs- und Dateisysteme sowie in weiterer Folge auch über Dateiformate ist ebenfalls essenzielle Voraussetzung für eine erfolgreiche Datenrekonstruktion bei Server- und Storage-Systemen.“ In fast allen Fällen ist eine erfolgreiche Datenrettung möglich. Für den Erfolg oder Misserfolg sind in der Regel die Folgeschritte entschei-



Der beste Schutz gegen einen fatalen Crash ist immer noch die Datensicherung – selbst wenn sie aufwändig und teuer ist.

dend, die noch unternommen wurden. So schwer es ist, der Schlüssel zu einer erfolgreichen Datenrekonstruktion liegt darin, im Notfall Ruhe zu bewahren. Dies erfordert vom IT-Leiter starke Nerven, berücksichtigt man die Tatsache, dass etwa Verwaltungsbereiche oder gar mehrere Stationen aufgrund eines Serverausfalls nicht mehr arbeiten können und jede Minute Geld kostet.

Richtig handeln, wenn Datenverlust aufgetreten ist

Für eine erfolgreiche Datenrettung gilt die Faustregel: So wenig Selbstversuche wie möglich am System vornehmen. Datenretter können so den Schaden mit vergleichsweise geringem Aufwand beheben und die Daten größtenteils oder sogar vollständig rekonstruieren. Zudem senkt es die Bearbeitungszeit und die daraus resultierenden Kosten. Insbesondere vom Einsatz semiprofessioneller Software ist abzuraten, aber auch das Ausführen eines CHKDSK ist mit Vorsicht zu genießen. Originaldaten werden hier umgeschrieben, was zur Folge hat, dass das Ergebnis der Datenrettung deutlich schlechter ausfallen kann, sollte das CHKDSK nicht ordnungsgemäß durchgelaufen sein. Datenretter führen die komplette Datenrettung bereits während der Diagnose durch und erkundigen sich explizit über den Ausfallhergang. Dabei gilt: Je spezifischer die Angaben dazu sind, desto leichter fällt es den Ingenieuren, die richtigen Verfahren anzuwenden. Das gilt für den Einsatz der verwendeten Hardware und für spezifische Informationen wie Raid-Level, Anzahl und Modellbezeichnung der Festplatten (mit Kennzeichnung der Slot-Nummer) sowie das verwendete Betriebs- und Dateisystem. Eine ordnungsgemäße Verpackung aller eingesetzten Datenträger klingt zwar selbstverständlich, wird laut Attingo jedoch des Öfteren unterlassen. Kommt es zur Datenrettung, dann sollte als Bemessungsgrundlage einzig der Aufwand der Datenrettung dienen. Kosten für Ersatzteile sollten nicht separat berechnet werden. Auch eine Abrechnung nach ge-



Wichtig bei der Datenrettung ist, dass IT-Leiter im Notfall Ruhe bewahren und umgehend professionelle Unterstützung anfordern.

retteten Gigabyte ist ebenso unseriös wie ein Angebot in Form eines Pauschalpreises. Gerade Pauschalpreise sehen auf dem ersten Blick attraktiv aus, haben aber zur Folge, dass Kunden fast immer zu viel zahlen. So ist das Pauschalangebot entweder übersteuert oder der Fall wird seitens des Datenretters aus wirtschaftlichen Gründen geschlossen, wenn der Pauschalpreis die erwarteten Kosten nicht deckt.

Das Erstellen von Backups und regelmäßige Disaster-Recovery-Tests minimieren das Risiko eines Datenverlusts erheblich. Da dies jedoch mitunter mit gewaltigen Kosten verbunden ist, die meist bei der Kostenstelle IT nicht eingeplant sind, wird auf diese Maßnahmen größtenteils oder sogar komplett verzichtet. Dann hilft möglicherweise nur noch die professionelle Datenrettung. ■

Kontakt

Attingo Datenrettung GmbH
 Andreas Mortensen
 Warnstedtstraße 12 B
 22525 Hamburg
 Tel.: 0 40 / 5 48 87 56-0
 Fax: 0 40 / 5 48 87 56-40
 a.mortensen@attingo.com
 www.attingo.com