Datenverluste in virtuellen Umgebungen – ein wachsendes Problem

Lösungen für eine zuverlässige Gewährleistung der Geschäftskontinuität

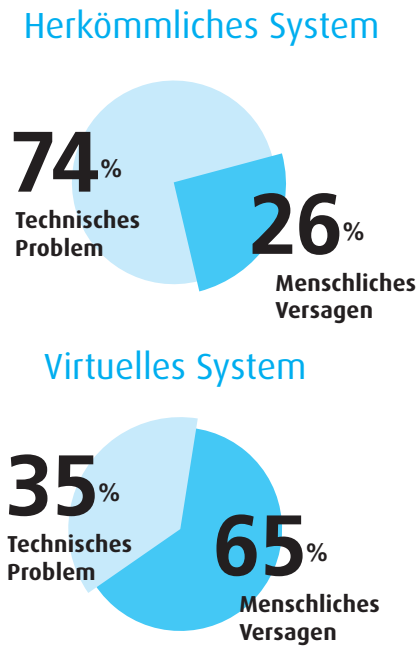
Kroll Ontrack

Einleitung

Oft sind die Begriffe „Geschäftskontinuität“ und „Notfallwiederherstellung“ in den letzten Jahren synonym verwendet worden. Dies hat bei Unternehmen für Verwirrung gesorgt, die ihren Geschäftsbetrieb schützen möchten. Ein Geschäftskontinuitätsplan stellt eine umfassende Richtlinie dar, mit der sichergestellt wird, dass alle Abteilungen eines Unternehmens bei Störungen möglichst ohne Beeinträchtigung weiterarbeiten können.[1] Ein Notfallwiederherstellungsplan ist mit seinen Maßnahmen in der Regel Bestandteil eines übergeordneten Geschäftskontinuitätsplans.

Durch den Einsatz von Virtualisierungstechnologie können viele Unternehmen Geschäftskontinuität planen und gewährleisten. Eine Virtualisierung ist jedoch hochkomplex und setzt bei IT-Mitarbeitern und Führungskräften besondere Kenntnisse und Fähigkeiten voraus. Bei einer nachlässigen Bereitstellung oder Verwaltung kann es passieren, dass Virtualisierung selbst geschäftliche Störungen oder Datenverluste verursacht (siehe Grafiken unten).

Bei einer nachlässigen Bereitstellung oder Verwaltung kann es passieren, dass Virtualisierung selbst geschäftliche Störungen oder Datenverluste verursacht.



Fehlerursache: Menschliches Versagen vs. technisches Problem

- Menschliches Versagen
- Mangelnde Schulung
- System- und Hardware-Fehler
- Extern (Stromausfall, Überspannung usw.)

(Abbildung 1)

Laut eines Berichts von Forrester Research zur Notallbereitschaft von Unternehmen (gemeinsam erstellt mit dem *Disaster Recovery Journal*)[2] haben viele Unternehmen ihre Notfallwiederherstellungslösungen in den letzten Jahren verfeinert. Trotz der wirtschaftlichen Probleme zeigten sich immer mehr Befragte zuversichtlich, auf Störungen im Rechenzentrum oder Ausfälle von Standorten vorbereitet zu sein.

76 % der Umfrageteilnehmer gaben an, in den letzten fünf Jahren von ernsthaften Ausfällen oder Störungen verschont geblieben zu sein. Forrester Research zufolge ist dies jedoch kein Grund zur Entwarnung. Ganz im Gegenteil: Rund 25 % aller Unternehmen hatten mit schwerwiegenden Problemen zu kämpfen.

---

[1] Im Sinne dieses Artikels sind Betriebsstörungen Vorfälle, die die Erledigung der täglichen Aufgaben behindern. Hierzu gehören Stromausfälle, gestörte Telefonleitungen usw. Als Datenverluste gelten Daten, die beschädigt sind. Somit gehören auch Datenverluste zur Kategorie Betriebsstörung.

[2] Bericht von Forrester Research aus dem Jahr 2010 zur Notfallbereitschaft von Unternehmen (gemeinsam erstellt mit dem Disaster Recovery Journal):http://www.drj.com/images/surveys_pdf/forrester/2011Forrester_survey.pdf

Außerdem sind Störungen des Geschäftsbetriebs deutlich häufiger als „erklärte Notfälle“. Es ist oft subjektiv, ob Unternehmen einen Notfall erklären oder nicht, meint Don Stewart, Director of Professional Services bei Ongoing Operations, einem gemeinnützigen Anbieter von Geschäftskontinuitätslösungen für US-amerikanische Genossenschaftsbanken. „Oft ist die IT-Abteilung so sehr mit der Lösung des Problems beschäftigt, dass die Geschäftsführung gar nicht über das Ereignis informiert wird“, berichtet Stewart. Manche Unternehmen haben gar nicht definiert, was eine Störung des Geschäftsbetriebs ist. So zögert die Führung, einen Notfall auszurufen, wenn das Ereignis als unbedeutend eingestuft wird. Beispiele hierfür wären der Ausfall des Telefonsystems oder Verzögerungen beim Versand und Empfang von E-Mails.

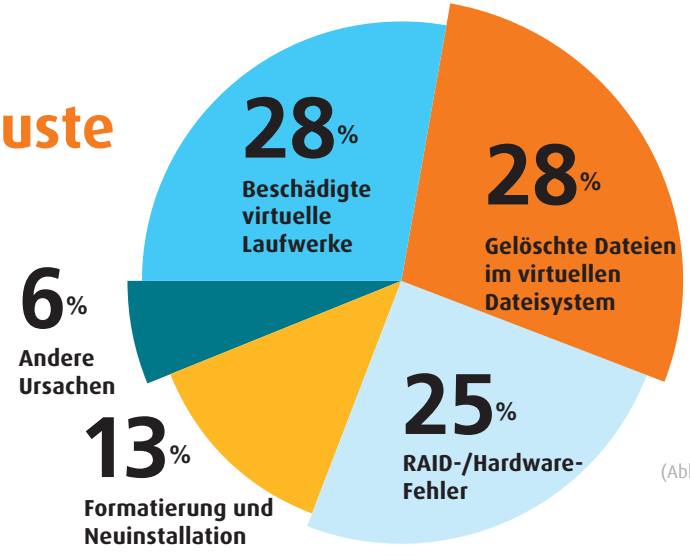
Lediglich 15 % der Befragten konnten die Kosten für einen Ausfall genau beziffern. Der erwartete Durchschnitt lag bei fast 145.000 USD pro Stunde.

Zur Vorbereitung auf Notfälle gehört mehr als ein dokumentierter Plan für Geschäftskontinuität. Erforderlich ist der Einsatz aller Beteiligten. Nur so kann sichergestellt werden, dass der Geschäftsbetrieb auch bei Störungen nicht beeinträchtigt wird. Stewart meint, dass eine Risiko- und Auswirkungsanalyse als Grundlage für einen effizienten Plan dienen sollte. Laut Stewart kaufen viele Unternehmen eine detaillierte Risikobewertung und belassen es dann dabei. „Der Bericht verschwindet in einem Schrank, ohne dass entsprechende Maßnahmen umgesetzt werden.“ Das ist ungefähr so effektiv wie die Erarbeitung einer Liste mit lebenswichtigen Gütern für den Brandfall, wenn die Liste niemals abgearbeitet wird.

Häufige Ursachen für virtuelle Datenverluste

Wenn es in virtuellen Rechenzentren zu Datenverlusten kommt, ist dies meist auf menschliches Versagen zurückzuführen. Virtuelle Datenverluste können aber auch mit Hardware-Fehlern zusammenhängen und durch fehlende Notfall-wiederherstellungspläne verschärft werden. Pläne, die zu ungenau sind oder nicht regelmäßig getestet werden, zwingen IT-Mitarbeiter dazu, ungetestete Reparaturen anhand unzulänglicher Vorschriften vorzunehmen. Selbstverständlich wünscht sich niemand einen Datenverlust oder eine Störung des Geschäftsbetriebs in seinem Zuständigkeitsbereich. So verlieren bei schwerwiegenden Datenverlusten oder Störungen des Geschäftsbetriebs oft alle verantwortlichen oder als verantwortlich deklarierten Mitarbeiter ihren Job.

Ursachen für virtuelle Datenverluste



(Abbildung 2)

Andere Datenverluste hängen mit einem zu hohen Vertrauen in die Redundanz von SAN-Systemen zusammen. Wertvolle Wiederherstellungszeit geht verloren, wenn mitten im Notfall erkannt wird, dass wichtige Sicherungskopien beschädigt oder nicht lesbar sind. Dies ist ein äußerst schlechter Zeitpunkt, um herauszufinden, dass Sicherungen nicht richtig ausgeführt worden sind oder die Sicherungssoftware Medienfehler nicht ordnungsgemäß gemeldet hat. Sehen Sie sich das von Kroll Ontrack bereitgestellte Kreisdiagramm an, in dem die Hauptursachen für virtuelle Datenverluste im Jahr 2010 aufgeführt sind:

Aktuelle Fallstudien zu Datenverlusten in virtuellen Umgebungen

Ein virtueller Datenverlust kann für Unternehmen katastrophale Folgen haben. Die finanziellen Auswirkungen von Störungen des Geschäftsbetriebs lassen sich nur schwer ermitteln. So spielen neben harten Faktoren wie Produktivitätsverlusten, verpassten Verkaufschancen und den Gehältern für Mitarbeiter auch weiche Faktoren wie mögliche Vertragsstrafen wegen fehlender Compliance, die Beschädigung des Unternehmensrufs und ein gesunkenes Kundenvertrauen eine Rolle. In der bereits erwähnten Umfrage von Forrester Research und DRJ konnten lediglich 15 % der Befragten die Kosten für einen Ausfall genau beziffern. Der erwartete Durchschnitt lag bei fast 145.000 USD pro Stunde. Diese Schätzung sollte jedem Geschäftsführer oder CIO Anlass genug sein, die Bereitschaft ihres Geschäftskontinuitätsplans zu überprüfen. Wie die folgenden Fallbeispiele zeigen, kann Virtualisierungstechnologie die Probleme zusätzlich erschweren.

Der Fall eines neu formatierten Servers

In einem italienischen Unternehmen kam es kürzlich zu einer Störung des Geschäftsbetriebs, als ein virtueller Host-Server mit 4 TB plötzlich nicht mehr auf das Speichersystem zugreifen konnte. Die virtuelle Umgebung umfasste 40 virtuelle Maschinen sowie verschiedene Betriebssysteme. Manche Geräte liefen mit Linux, andere mit älteren UNIX-Systemen, und der Rest bestand aus Microsoft® Windows®-Servern. Hiermit wurden die Anwendungs-, Web- und Datenbankserver unterstützt.

Nur branchenweit akzeptierte Best Practices und eine zuverlässige IT-Verwaltung sorgen für höchste Datensicherheit.

Der virtuelle Host-Server wurde als Linux-basierter Hypervisor mit zwei verknüpften 2-TB-LUNs betrieben. Eines Tages wurden die Speicher-LUNs neu formatiert. Der Grund für die Neuformatierung wurde nicht mitgeteilt, doch der Schaden an den vorhandenen Dateisystemstrukturen war immens. Bei der Neuformatierung schreibt der Speichermanager von Linux im gesamten Volume Metadaten des EXT-Dateisystems in vordefinierte Bereiche. Diese Metadaten enthalten lediglich ein paar Tausend Byte an Informationen. Dennoch waren die Auswirkungen auf das Dateisystem des virtuellen Host-Servers sowie auf die virtuellen Laufwerksdateien verheerend.

Jede virtuelle Maschine verfügte über vier bis sechs virtuelle Laufwerksdateien, so dass auf dem Host-Server 70 bis 90 virtuelle Laufwerksdateien gespeichert waren. Manche der virtuellen Microsoft Windows-Server wiesen Konfigurationen mit dynamischen Laufwerksvolumes (per „Logical Volume Manager“ in Linux) zwischen verschiedenen virtuellen Laufwerksdateien auf, was die Wiederherstellung weiter erschwerte.

Nachdem die IT-Abteilung des Unternehmens ihre internen Möglichkeiten erschöpft hatte, wurde ein professioneller Anbieter von Datenrettungsservices mit der Wiederherstellung der Daten beauftragt. Trotz der Beschädigungen konnten virtuelle Laufwerksdateien gefunden und wichtige Daten wiederhergestellt werden.

Der Fall einer desaströsen Datenzusammenführung

Bei einer Fusion in den USA kam es zu einem Desaster, als die IT-Abteilungen der beiden Unternehmen ihre Daten zusammenführten. Ursache war wahrscheinlich Sabotage durch einen Mitarbeiter. Der Fall wird noch von Computerforensikern untersucht.

Der virtuelle Host-Server des ersten Unternehmens umfasste über 400 virtuelle Maschinen in 20 Speicher-LUNs. Bei der Datenzusammenführung löschte ein Mitarbeiter mit Administratorzugriff auf den virtuellen Host-Server systematisch alle 400 virtuellen Maschinen sowie die virtuellen Laufwerksdateien. Dabei gingen über 440 virtuelle Laufwerksdateien sowie mehr als 1.000 Snapshot-Dateien verloren.

Das verschmelzende Unternehmen beauftragte umgehend einen Anbieter von Datenrettungsservices mit der Wiederherstellung der zentralen Server, auf denen essentielle Dienste bereitgestellt wurden. Nach drei Tagen waren diese Systeme wieder verfügbar. In den folgenden zwei Wochen wurde auch das restliche Speichersystem wiederhergestellt. In einem aufwändigen Verfahren wurden nicht zugewiesene Bereiche des Speicher-LUNs auf mögliche virtuelle Laufwerksdateien untersucht, die sich nur anhand ihrer Dateisystemattribute erkennen lassen.

Durch eine Wiederherstellung von Sicherungskopien sowie der ursprünglichen Volumes konnten die Daten gerettet werden. Die meisten virtuellen Laufwerksdateien waren vollständig. Bei manchen virtuellen Laufwerken mussten jedoch aufgrund der Beschädigung des Dateisystems die Dateiinhalte extrahiert werden.

Der Fall einer SAN-Neuformatierung an einem externen Standort

In einem Unternehmen aus Luxemburg ging bei der Notfallwiederherstellung alles schief. Bei der Routinewartung des SAN-Speichers für die virtuellen Maschinen des Unternehmens wurde das SAN aus Versehen auf einen anderen physischen Server geleitet. Als der SAN-Speicher als „unbekannt" identifiziert wurde, erfolgte eine Neuformatierung des Volumes. Zuerst befürchtete das Personal einen möglichen Datenverlust. Die Mitarbeiter waren erleichtert, als sie sich an den identischen SAN-Speicher an einem externen Standort erinnerten, der über eine Technologie für die automatische Standort-Replikation verfügte. Vielleicht würde es sich doch nur um eine kleine Geschäftsstörung handeln.

Doch nach der Anmeldung am Remote-SAN erkannte das IT-Team, dass es sich bei dem Remote-SAN um eine identische Kopie des primären Standorts handelte.

Vor der Wartung war die Technologie für die automatische Standort-Replikation leider nicht deaktiviert worden. So wurde im Zuge der Neuformatierung am primären Standort auch das sekundäre SAN neu formatiert. Durch den Einsatz erfahrener Datenrettungsexperten konnten die virtuellen Maschinen und virtuellen Laufwerksdateien erfolgreich wiederhergestellt werden.

Das Unternehmen verfügte über keinerlei Sicherungskopien, da man davon ausgegangen war, dass die duale Speicherarchitektur sowie das Verfahren für die Standort-Replikation ausreichend Daten- und Systemredundanz bieten würden. Dieser Fall ist besonders lehrreich, da die Funktionen der Speicherausrüstung das Unternehmen in falscher Sicherheit wiegten. In Wirklichkeit sorgen jedoch nur branchenweit akzeptierte Best Practices und eine zuverlässige IT-Verwaltung für höchste Datensicherheit.

Konsequenzen von Datenverlusten

Virtualisierung hat die IT-Branche revolutioniert und zeichnet sich durch niedrigere Anlagen- und Ausrüstungskosten aus. Laut einer weltweiten IDC-Analyse externer Laufwerkspeichersysteme betrug die Gesamtkapazität der ausgelieferten Laufwerkspeicher mehr als 5.100 Petabyte – eine Steigerung um 55,7 % im Vergleich zum Vorjahr.[3] Angesichts dieses Wachstums ist eine zuverlässige IT-Verwaltung mit einer ausführlichen Dokumentation der Notfallwiederherstellung sowie regelmäßigen Übungen der Notfallpläne erforderlich. Nur so lassen sich Störungen des Geschäftsbetriebs, die mit Datenverlusten in virtuellen Umgebungen zusammenhängen, wirkungsvoll minimieren bzw. ganz verhindern.

Je mehr Speicher durch Virtualisierungstechnologie genutzt wird, desto wichtiger werden die Verwaltung und der Schutz der virtuellen Ressourcen. Die Sicherstellung der Geschäftskontinuität auf Grundlage intelligenter und ausführlich getesteter Wiederherstellungspläne ist unerlässlich.

Erfolgreiche Unternehmen wissen, dass jede Störung in der virtuellen Infrastruktur – und sei sie noch so klein – den gesamten Geschäftsbetrieb beeinträchtigen kann. Darum haben viele IT-Führungskräfte und Planer von Geschäftskontinuitätslösungen Datenrettungsservices proaktiv in ihre Notfallpläne integriert. Wenn IT-Teams einen geeigneten Anbieter von Datenrettungsservices wählen, bevor es zu tatsächlichen Störungen kommt, können sie Probleme im Geschäftsbetrieb verhindern, die mit Datenverlusten zusammenhängen.

[3] Worldwide Disk Storage Systems Finishes 2010 with Double-Digit Growth on Strong Fourth Quarter Results, IDC, März 2011

Kroll Ontrack

Mehr Informationen im Internet oder
über unsere kostenlose Hotline:

0800 10 12 13 14

www.krollontrack.de