Datenverfügbarkeit sichern

DATA/IT ■ Speziell in der datenintensiven Druck- und Medienindustrie würde heute kaum noch jemand die große Bedeutung von Datenschutz und -sicherheit in Abrede stellen. Trotzdem hat die von kleinen und mittleren Betrieben geprägten Branche immer noch erstaunlich große Baustellen beim Datenmanagement, vor allem in den Bereichen IT Business Continuity und Desaster Recovery. Strategien für die letzten Prozentpunkte Ausfallsicherheit erfordern eben große Anstrengungen und verursachen hohe Kosten. Doch was davon macht für diese Unternehmen überhaupt Sinn?

■ Business Continuity ist eine Managementaufgabe und folgt natürlich auch betriebswirtschaftlichen Aspekten. Von daher müssen die Aufwände immer gegen die Kosten gerechnet werden, die etwa Betriebsunterbrechungen, Produktionsausfälle oder gar Vertragsstrafen verursachen könnten. Zudem kann ein Ausfall im IT-Bereich oder der Verlust von Daten auch Renommee kosten. Die Frage ist also stets, welche Konsequenzen der Ausfall von produktionskritischen Ressourcen hat: Wie lange kann ich einen Produktionsstillstand hinnehmen, was passiert wenn Kundenaufträge nicht angenommen werden können?

Business Continuity Management (auf Deutsch: betriebliches Kontinuitätsmanagement) ist der Terminus für die Sicherstellung des alltäglichen Betriebs, dessen Unterbrechung eine Katastrophe darstellt, die wiederum durch Desaster Recovery zu beheben ist. Dieser Artikel setzt sich mit den technischen Herausforderungen und Strategien im Zusammenhang mit Business Continuity/Desaster Recovery im IT-Bereich auseinander.

BUSINESS CONTINUITY MANAGEMENT. Eine Strategie gegen Ausfälle des eigenen Equipments ist die Auslagerung von Hardware und Daten in die Cloud. In den Rechenzentren der Cloudanbieter und auch der Hoster, die lediglich Rechen- und Speicherkapazität anbieten, wird großer Aufwand betrieben, um Ausfallsicherheit zu gewährleisten. Redundante Internetanbindung, Servercluster, automatisierte Backuproutinen und Ähnliches lassen sich (in Relation zu den Kosten im eigenen Serverraum) zu vertretbaren Kosten anmieten. Allerdings reagieren Kunden aus der Industrie, dem Versicherungs- und Bankenwesen mitunter empfindlich auf die Lagerung ihrer schützenswerten Daten bei Dritten. Zu beachten ist zudem, welche Bandbreiten vorgehalten werden müssen, um den Traffic zwischen dem Hoster und dem Produktionsstandort zu bewältigen. Daher werden häufig nur die Internetpräsenz und die Webshops auswärts gehostet, während die Verarbeitung von Druckdaten weiter lokal stattfindet.

AUFBAU VON REDUNDANZ. Wer sich Gedanken um Ausfallsicherheit macht, ist gut beraten, zunächst die kritischen und ausfallgefährdeten Komponenten zu identifizieren. Festplatten und Netzteile etwa sind solche Komponenten, die sich relativ einfach redundant auslegen lassen. Anstatt viele Festplatten „einfach so“ zu betreiben, lassen sie sich mit geeigneter Hard- oder Software zu RAIDs zusammenschließen, die je nach RAID-Level den Ausfall einer oder gar mehrerer Festplatten ohne Betriebsunterbrechung und Datenverlust ausgleichen können. Ist in einem solchen RAID ein einzelnes Netzteil verbaut, sorgt dessen Ausfall für Betriebsunterbrechung und evtl. auch Datenverlust, weshalb im Profibereich stets mindestens zwei Netzteile verbaut werden. Diese Beispiele sollen stellvertretend für die Strategie stehen, Single Points of Failure (SPoFs) zu vermeiden. Einfache Redundanz hilft bereits enorm, noch ausgefuchstere Systeme weisen mehrfache Redundanzen auf, bzw. werden als komplette Systeme parallel betrieben. Fällt eines aus, übernimmt ein anderes die Aufgaben des ausgefallenen (Fail Over).

Blick auf die virtuelle Umgebung im Serverraum von CTRL-S. Im Bild unten der Cluster aus ESX-Hosts und darüber das SAN (Storage-Area-Network).

Redundanz in örtlicher Nähe hilft nichts, wenn zum Beispiel beide Komponenten an diesem Ort durch Brand oder Stromausfall ausfallen. Will ich SPoFs vermeiden, müssen nicht nur die IT-Kernkomponenten, sondern auch die Peripherie (Klimaanlagen, Stromversorgung, Internet etc.) redundant ausgelegt sein. Hier wird klar, dass die letzten paar Prozentpunkte Ausfallsicherheit am meisten Geld kosten. Ein zweites Netzteil für einen 5 000-Euro-Server kann für 250 Euro angeschafft werden, das RAID-System kostet allerdings häufig um Einiges mehr. Will ich Redundanz, muss ich nicht nur die Hard-, sondern auch die Software redundant auslegen. Interessant werden hier die Lizenzbedingungen der Softwarehersteller, für die selbstredend nicht zu durchschauen ist, ob nun ein Unternehmen die Software „just in case“ am zweiten Standort vorhält oder täglich produktiv betreibt. Sind gar Dongles im Form von Hardware vorhanden, ist der doppelte Kauf der Software unumgänglich, wenn zum Beispiel der Ausfall in Folge eines Brandes im Serverraum minimiert werden soll. Hundertprozentige Sicherheit ist unbezahlbar. Komplette Systeme an unterschiedlichen Standorten mehrfach redundant auszulegen (beachte: auch die Breitbandverbindungen zwischen den Standorten müssen mehrfach redundant sein!), ist für das typische Medienunternehmen nicht zu finanzieren. 98% Verfügbarkeit bedeuten bereits 7,3 Tage Ausfall im Jahr. Irgendwo dazwischen sollte man sich bewegen.

SYSTEMMONITORING. Aber auch mitunter wenig bedachte Problemchen können ärgerliche Ausfälle produzieren. Ein typisches Beispiel kann das Zulaufen einer Systempartition auf einem wichtigen Server sein. War ursprünglich nach der Installation von Betriebssystem und Anwendungssoftware noch jede Menge „Luft“ vorhanden, ist nach einigen Updates oder dem unglücklichen Anlegen einer Printer-Queue kein weiterer Platz mehr da. Der Server schmiert ab und ist erst nach dem Einsatz des Systemadministrators wieder flott zu kriegen. Abhilfe können hier Monitorsysteme schaffen, die alle kritischen Komponenten überwachen und rechtzeitig beim Erreichen des eingestellten Schwellenwertes der Festplattennutzung den Systemadministrator benachrichtigen. Solche Monitorsoftware (etwa den Klassiker Nagios) gibt es kostenlos, der Aufwand zur Einrichtung und ständigen Pflege in den sich dynamisch ändernden Systemlandschaften moderner Medienunternehmen ist aber nicht zu unterschätzen.

DESASTER RECOVERY MANAGEMENT. Desaster Recovery (auf Deutsch: Notfallbehebung) ist ein Bestandteil der Business Continuity. Wie der Name schon sagt, sollen beim Eintritt von nicht zu vermeidenden Unglücken Szenarien greifen, die zur schnellstmöglichen Wiederaufnahme des unterbrochenen Betriebes führen.

Einen wesentlichen Baustein in dieser Strategie stellt das Backup dar. Im professionellen Bereich kann hier sinnvollerweise nur automatisiert vorgegangen werden. Es ist zwischen dem Backup des Contents (der Nutzdaten) und des Rechners zu unterscheiden. Letzteres wird in der Regel durch ein Image des Systemdatenträgers durchgeführt, ersteres im einfachsten Fall durch Kopieren der Dateien. Der Content eines einzelnen Rechners

DD-SERIE

DATENMANAGEMENT IN DER PRAXIS

In enger Zusammenarbeit mit dem Prepress-Spezialisten CTRL-S GmbH (Stuttgart) zeigt *Deutscher Drucker* auf, wie ein professionelles Datenmanagement bei Mediendienstleistern heutzutage aussehen kann.

- Teil 1 (Desaster Recovery/Business Continuity) in dieser Ausgabe,
- Teil 2 (Datenschutz) folgt in DD 6/2015,
- Teil 3 (Produktionssicherheit/Datenqualität) folgt in DD 8/2015

kann meist mit Bordmitteln gebackupt werden, bei einer Serverfarm sollte das von speziellen Systemen, die auch das Backup laufender Datenbanken erlauben, erledigt werden.

ÖRTLICHE TRENNUNG! Der Ort, an dem die Backup-Medien gelagert werden, sollte außerhalb des Standortes, wenigstens aber in einer anderen Brandschutzzone desselben Gebäudes liegen. Denn die Katastrophe wird vollkommen, wenn sie neben dem Content auch die Backups vernichtet. Die in der Vergangenheit heiß diskutierte Frage, ob das Backup auf Bänder oder auf Festplatten erfolgen soll, ist inzwischen zu einer Kapazitäts- und Kostenfrage geworden. In punkto Schreib- und Lesegeschwindigkeit sind moderne Tape- und Disksysteme einander ebenbürtig. Die heute üblichen Datenmengen erfordern robotergesteuerte Tape-Libraries oder RAID-Systeme als Backup-Hardware. Die erforderliche Kapazität errechnet sich aus der Menge der täglich zu sichernden Daten mal der Menge der aufzubewahrenden Sicherungsläufe und beträgt infolgedessen ein Vielfaches des Online-Speichers der produktiven Systeme. Moderne Backupsysteme erlauben die Definition eines Schreibschutzes auf die Backupmedien für eine gewisse Zeit oder für eine definierte Zahl an Sicherungsläufen. Danach werden die Medien zum Überschreiben freigegeben. Ein gut eingerichtetes Backupsystem kann daher nahezu wartungsfrei über längere Zeiträume laufen und informiert die Verantwortlichen im Fehlerfall.

Bei der Wahl der Backup-Strategie müssen die Zeitfenster, in denen das Backup möglich ist, genauso berücksichtigt werden, wie das gewünschte Zeitfenster zur Wiederherstellung. Eine beliebte Backup-Strategie ist zum Beispiel die Vollsicherung am Wochenende und eine differenzielle Sicherung in jeder Nacht. Bei der differenziellen Sicherung wird immer die Differenz zum letzten Full Backup gesichert, das heißt im Desasterfall müssen lediglich die letzte Voll- und die letzte differenzielle Sicherung eingespielt werden, um den Zustand des Vortages wiederherzustellen. Maschinenimages von Workstations oder Servern, die einzeln auf dedizierten Hardwareplattformen laufen, lassen sich in der Regel nur auf Rechner mit identischer Hardware zurückspielen. Bei Hardwareausfall kann das Image nicht ohne Aufwand auf einen beliebigen – ggf. moderneren und leistungsfähigeren Rechner – zurückgespielt werden.

VIRTUELLE MASCHINEN. Einfacher geht das bei virtuellen Systemen, die auf hochleistungsfähiger Hardware eine Softwareschicht bereitstellen, die Hardware simuliert und auf der Workstations und Server mit unterschiedlichen Betriebssystemen als VMs (Virtual Machines) installiert werden können. Eine solche virtuelle Umgebung wird Host genannt. Leistungsfähige Hosts für virtuelle Maschinen können zunächst vergleichsweise günstig sein, aber auch dort sind Ausfallsicherheit und Redundanzen mit Kosten verbunden. Die Entscheidung für virtuelle Umgebungen ist also nicht in erster Linie eine kostengetriebene. Weil in der virtuellen Umgebung nur virtuelle Hardwarekomponenten existieren, kann ein Image der Maschine sogar auf einen anderen Host zurückgespielt werden. Mehrere Hosts können zu einem Cluster zusammengeschlossen werden und Hochverfügbarkeits-Optionen sorgen dafür, dass beim Ausfall eines Hosts oder auch nur temporär hoher Last auf diesem Host, VMs im laufenden Betrieb auf andere Hosts verschoben werden. Voraussetzung dafür: Trennung von Rechenkapazität und Speicherplatz! Physikalisch liegen Rechner (die in virtuellen Umgebungen auch nur Daten sind) und Daten auf Storagesystemen (SAN), die durch ein Hochgeschwindigkeitsnetz mit den Hosts, die nur Arbeitsspeicher und Rechenkapazität zur Verfügung stellen, verbunden sind. Sehr moderne Systeme replizieren fortwährend auf ein zweites System, das im Desasterfall ohne Datenverlust und zeitliche Verzögerung zur Verfügung steht.

ZENTRALE BEREITSTELLUNG. Applikationen und Desktops werden heute wieder zentral bereitgestellt. Application- und Terminalserver sind ebenfalls Virtualisierungstechniken, die mit der Bereitstellung von Arbeitsplätzen und Applikationen in der Cloud auf die Spitze getrieben werden. Höchste Ansprüche an Datenschutz erfüllen private Clouds, die ein Unternehmen für seine Mitarbeiter unter scharfer Zugangskontrolle zur Verfügung stellt. Für Windows und Linux existieren unterschiedlichste Terminalserver-Technologien (zum Beispiel von Citrix, Microsoft, VMware), in der Apple-Welt hinkt man noch etwas hinterher. Nach den Erfahrungen von CTRL-S sind auch anspruchsvolle Applikationen wie Layoutprogramme, PDF-Workflowssysteme, Seitenmontage und einfache bis mittelkomplexe Bildbearbeitung auf Terminalservern möglich, lediglich die Reproabteilung bleibt bei hoch anspruchsvoller Bildbearbeitung lieber auf der lokalen, farbverbindlichen Workstation. Natürlich stellt auch ein einzelner Terminalserver einen SPoF dar, dem aber wiederum durch Terminalserverfarmen, also Redundanz, entgegengewirkt werden kann und muss. Die Verlagerung der Hard- und Software ins Rechenzentrum bringt den Systemadministratoren klare Vorteile und schont die Turnschuhsohlen. Die Thin Clients auf den Schreibtischen der User können nichts weiter als zu den Servern verbinden, Pflege- und Konfigurationsaufwand ist für diese Komponenten praktisch gleich Null.

Backupsysteme sind bei CTRL-S räumlich getrennt in einem zweiten Serverraum untergebracht.

DEN ERNSTFALL ÜBEN. Notfallpläne sind gut und notwendig, gut schlafen können verantwortungsvolle Administratoren aber nur dann, wenn die Katastrophe und die in den Notfallplänen vorgesehenen Maßnahmen regelmäßig geübt werden. Dabei sollte ein Katastrophenszenario so realistisch wie möglich simuliert werden. Technisch erfordert das Nacht-, Feiertags- oder Wochenendarbeit, es muss in jedem Fall ein ausreichender Zeitpuffer zur Verfügung stehen, damit sich die Übung auch beim Eintritt von nicht im Notfallplan bedachten Ereignissen nicht zum Ernstfall entwickelt. Notfallpläne sollten immer auch organisatorische Fragen stellen und beantworten: Welche Mitarbeiter werden benötigt, stehen sie im Notfall zur Verfügung, wie sind sie erreichbar, wie ist ihre Vertretung geregelt? Benötige ich Hilfe von Dienstleistern, sind die dafür abgeschlossenen SLAs (Service Level Agreements) ausreichend? Sind weitere Partner einzubinden, die ggf. Teile der Produktion übernehmen können?

FAZIT. Für Business Continuity Management und Desaster Recovery Management gibt es keinen Königsweg. Jeder Betrieb ist anders, viele Strategien sind denkbar und zwischen Mut und Unvernunft läuft keine klare Linie. Wer über interne Kompetenz verfügt, sollte diese regelmäßig überprüfen und den Ernstfall proben. Wer nicht, sollte sich nach kompetenter Hilfe umsehen. Hier den richtigen Partner zu finden oder die Balance zwischen Kosten und Nutzen zu halten, ist schwierig. Wegen der längst noch nicht abgeschlossenen Digitalisierung sollte sich das Management eines Medienunternehmens aber verpflichtet fühlen, sich der genannten Problematik zu öffnen.

Für viele Medienunternehmer ist noch immer die zentrale Frage, was gekauft werden soll. Entscheidender für den Erfolg und das Bestehen des Unternehmens dürfte aber vielmehr die Frage sein, wie das Gekaufte betrieben wird. Und über dieses „Wie“ entscheiden auch die Mitarbeiter in den Unternehmen mit, deren Motivation und Disziplin für die Umsetzung der Themen, die wir in den kommenden Folgen dieser Artikel-Serie behandeln, von größter Bedeutung sind. **(ms)**