Herausgegeben von Acronis

Acronis Sonderedition

Backup

FÜR DUMMIES®

Auf einen Blick:

- Antworten auf häufige Fragen zu Backup und Recovery
- Zehn Tipps für einfacheres Backup und Recovery
- Wie Sie auch moderne Data Protection meistern, selbst bei Virtualisierung, Cloud und Datenwachstum

Joel Berman
Spezialist bei Acronis

Acronis

Backup & Storage Management für Unternehmen

Produkte und Lösungen für beliebige Umgebungen

Acronis bietet erstklassige Data Protection der Neuen Generation für virtuelle, physische, mobile und Cloud-Umgebungen

Basierend auf der **AnyData Engine**, bietet Acronis einfach zu bedienende und umfassende Lösungen für Backup, Disaster Recovery und sicheren Zugriff. Als eines der weltweit führenden Unternehmen im Bereich Data Protection und Systemverwaltung, bieten wir viele technologische Vorteile:

Eine preisgekrönte Backup-Technologie, die *alle Daten* in einem einzigen, einfachen Schritt sichert.

Ultraschnelles Disaster Recovery, das Sie in wenigen Minuten wieder einsatzbereit macht

Flexible Wiederherstellungsoptionen, von einzelnen Dateien bis zum vollständigen Server

Multidestination Backup, das die gesicherten Daten an beliebigen Zielorten (einschließlich der Acronis Cloud) ablegen kann

Tools für Systemdeployment in einem Schritt ermöglichen eine schnelle und kosteneffiziente Systempflege

Hilfreiche Tools zur Festplattenverwaltung, um IT-Tasks zu optimieren und die System-Performance zu verbessern

Software, die speziell für einfache Bedienbarkeit entwickelt wurde und so gut wie selbsterklärend ist

Zentrale Verwaltung und einfaches Reporting über eine leicht zu bedienende Konsole

Laden Sie eine kostenlose Testversion der Acronis Backup- und Recovery-Software herunter!
Besuchen Sie www.acronis.com/de-de/backup/free-trials

Acronis

Backup

FÜR

DUMMIES®

Acronis Sonderedition

von Joel Berman

WILEY

Backup Für Dummies®, Acronis Sonderedition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-10184-0 (pbk); ISBN: 978-1-119-10179-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Johnson
Development Editor: Kathy Simpson
Acquisitions Editor: Katie Mohr
Editorial Manager: Rev Mengle
Business Development Representative: Sue Blessing
Custom Publishing Project Specialist: Michael Sullivan
Production Coordinator: Melissa Cossell

Inhaltsverzeichnis

Einführung

Viele Computernutzer denken, dass es beim Thema „Backup“ lediglich darum geht, Daten zu kopieren – und diese dann irgendwann einmal bei Bedarf auf dem ursprünglichen System (oder einem Ersatzsystem) durch simples „Zurückkopieren“ wiederherzustellen. In den 60er Jahren des vergangenen Jahrhunderts war ein solcher Backup-Prozess möglicherweise auch wirklich noch so einfach. Als Backup-Prozess stanzte man damals einfach einen weiteren Satz Lochkarten, die anschließend an einem sicheren Ort aufbewahrt wurde – fertig!

Tja, damals war die (digitale) Welt noch einfach. In den vergangenen 50 Jahren hat die Entwicklung der IT-Technik aber große Fortschritte gemacht – und so mussten sich folglich auch alle Prozesse rund um das Thema „Backup und Wiederherstellung“ weiterentwickeln. Backups umfassen eine Vielzahl von Anwendungsfällen! Das beginnt bei einer einfachen Dateiwiederherstellung durch Kopieren – kann aber auch bis zur Wiederherstellung sehr komplexer Systeme reichen, die sogar aus vielen Maschinen bestehen können.

Übrigens verwende ich den Begriff „Maschine“ hier als Überbegriff für PCs und Computer, da es mittlerweile neben den klassischen physischen Computern auch virtuelle Computer gibt, die man üblicherweise als virtuelle Maschinen (VMs) bezeichnet.

Über dieses Buch

Ein Backup und eine Wiederherstellung so durchzuführen, dass man lediglich schnell ein paar Dateien auf ein anderes Laufwerk kopiert (und diese im Bedarfsfalle dann ebenso einfach wieder zurückkopiert), ist wirklich nur für sehr einfache Fälle eine zufriedenstellende Lösung. Die in diesem Buch behandelten Anwendungsfälle erstrecken sich daher von einfachen, einzelnen Computern bis hin zu großen und komplexen Systemen aus vielen Maschinen.

Der Begriff „Datensicherung“ (DS) ist ein Oberbegriff für die Sicherung (in Form von Backups) und Wiederherstellung aller möglichen Arten von Informationen. Dazu gehören nicht nur einfache (Daten)Dateien, sondern eben auch

Anwendungsprogramme oder die Betriebssystem-Software. Der Begriff „Datensicherung“ wird leider häufig mit dem Begrif „Datensicherheit“ verwechselt. Bei letzterer geht es sich jedoch eher um den Schutz kritischer Daten (z. B. persönlicher Kreditkarteninformationen) vor einem unberechtigten Zugriff. Datensicherheit erreicht man beispielsweise durch die Verschlüsselung von Daten. In diesem Buch beschäftigen wir uns aber mit der Sicherung von Informationen/Daten durch Backup- und Wiederherstellungsprozesse. Ein weiteres, häufig auftauchendes Schlagwort ist „Disaster Recovery“ (abgekürzt DR, hier in der mittlerweile gängigeren englischen Schreibweise verwendet). Unter Disaster Recovery versteht man die Wiederherstellung wichtiger Daten oder eines kompletten Systems nach einem größeren und unerwarteten Schaden. Ein solcher Schaden kann an der Hardware des Systems erfolgen (z. B. durch Blitzeinschlag, Überschwemmung etc.) oder auch an der Software (z. B. durch einen Hacker-Angriff, bei dem das System mit Viren infiziert wird).

Dieses Buch ist also Ihr Leitfaden zum Thema „Datensicherung“.

Annahmen über den Leser

Als ich dieses Buch schrieb, ging ich von Folgendem im Hinblick auf Sie, werter Leser, aus:

- Sie sind zwar grundsätzlich mit moderner Informationstechnologie (IT) vertraut, aber kein Experte für Datensicherung.
- Sie kennen sich ein wenig mit der Verwaltung von Systemen aus, sind jedoch kein erfahrener Systemadministrator.
- Im Wesentlichen ging ich davon aus, dass Sie (ob nun privat für sich oder für Ihr Unternehmen) neue Backup-Prozesse einführen oder bereits bestehende Prozesse verbessern möchten. Desweiteren ging ich davon aus, dass Sie Hilfe beim tieferen Verständnis der grundlegenden Konzepte, der Auswahl geeigneter Backup-Produkte und der Etablierung einer gut funktionierenden Datensicherungslösung suchen.

Symbole in diesem Buch

Wie in allen ... *für Dummies*-Büchern weisen Symbole am Seitenrand auf bestimmte Arten von Informationen hin.

Textpassagen, die mit diesem Symbol gekennzeichnet sind, enthalten nützliche Tipps zu Backup-Konzepten oder -Techniken.

Dieses Symbol weist auf wichtige Information hin, die es wert sind, im Gedächtnis behalten zu werden.

Abschnitte mit diesem Symbol („Technikkram“) müssen Sie dagegen nicht unbedingt lesen. Ich hoffe aber, dass Sie es dennoch tun – denn Sie erhalten dadurch ein tieferes Verständnis der Prozesse rund um das Thema Backup.

Passagen, die mit dem Symbol „Warnung“ gekennzeichnet sind, sollten Sie besser nicht überspringen. Solche Warnungen nicht zu beachten, könnte Sie sonst im ungünstigsten Fall Zeit, Geld und/oder Daten kosten.

Wie es weitergeht

Wie alle ... *für Dummies*-Bücher kann auch dieses in beliebiger Reihenfolge gelesen werden. Egal, ob Sie mit Kapitel 1 beginnen wollen, um sich chronologisch durch das Buch zu arbeiten – oder ob Sie das Querlesen bevorzugen: Sie entscheiden, auf welche Weise Sie vorgehen wollen.

Kapitel 1

Einführung in die Datensicherung

In diesem Kapitel

- Warum müssen Daten gesichert werden?
- Welche Daten müssen gesichert werden?
- Was gehört zu einem Backup-System?

Unternehmen haben ihre Daten schon immer gesichert. Im letzten Jahrhundert wurden beispielsweise Kohlepapierdurchschläge in Lagerhäusern aufbewahrt (und vielleicht passiert das bei manchen Unternehmen auch noch heute ;-)). Seitdem haben sich die Zeiten jedoch für die meisten Anwender deutlich geändert. Die Techniken, um Informationen per Backup zu sichern und dann bei einem katastrophalen Datenverlust wiederherstellen zu können, haben sich stark entwickelt. Dieses Kapitel bringt Sie im Hinblick auf moderne Datensicherung auf den neuesten Stand.

In diesem Buch bedeutet der Begriff *Datensicherung* eine Sicherung von Daten über einen Backup-Prozess, der üblicherweise in der Erstellung von Dateien resultiert, die Backup-Archive genannt werden. Diese Backups müssen ein einfaches Durchsuchen und Wiederherstellen der Daten ermöglichen – unabhängig davon, wo genau in den Backup-Archivdateien sich die gesicherten Daten befinden. Der ergänzende, hier oft verwendete Begriff *Disaster Recovery* bezeichnet schließlich die schnelle Wiederherstellung von gesicherten Daten nach einem schwerwiegenden Problem. Bei den wiederhergestellten Daten kann es sich wichtige Dateisammlungen handeln – aber auch um komplette Systeme (egal ob Arbeitsstation, Server oder sogar ein komplettes Rechenzentrums).

Den Begriff „Daten" definieren

Was genau (in diesem Kontext) sind eigentlich „Daten"? Die Frage erscheint zuerst recht einfach; leider ist es die richtige Antwort aber nicht. Daten können sehr unterschiedlich sein. Beispielsweise einfache

Textdateien – aber auch sehr verschiedenartige und komplexe Informationen. Auf modernen Computersystemen und in diesem Buch werden im Wesentlichen drei Arten von Daten verwendet: Dateien, Metadaten und Programme.

Da diese Datentypen sehr viele Formen annehmen können, ist es nicht immer leicht, zu erkennen, welche Daten genau (und auf welche Art) gesichert werden müssen, damit die spätere Wiederherstellung (beispielsweise des Betriebssystems) auch erfolgreich ist. Ganz grundsätzlich gilt: alles was einen Wert hat, sollte möglichst auch gesichert werden. Und je höher der Wert, desto wichtiger die Sicherung. Genauso wie prähistorische Menschen sicherlich darauf achtgaben, ihre Kinder von Säbelzahntigern fernzuhalten, achten Sie sicherlich auch darauf, wo Sie eine teure Uhr ablegen oder Ihr Auto parken. Wenn solche physische Gegenstände verloren gehen oder gestohlen werden, verlieren Sie oft auch einen mit den Gegenständen verbundenen Wert. Klassische Versicherung können nur mit Geld entschädigen – der verlorene Gegenstand selbst kann zumeist nicht wiederbeschafft werden.

Mit den digitalen Daten eines Computersystems verhält es sich aber anders! Im Gegensatz zu physischen Gegenständen können digitale Daten kopiert werden. Dabei bleiben üblicherweise auch alle mit ihnen verbundenen Werte erhalten. So etwas wie ein „Original“ gibt es bei digitalen Daten nicht mehr ohne weiteres. Wenn Sie Ihre Daten und deren Datensicherungen gut pflegen, ist eine Wiederherstellung recht einfach. Dabei wird dann auch der ursprüngliche Wert der Daten mit wiederhergestellt.

Daten sichern

Anwender mit Computer-Erfahrung (nennen wir Sie mal IT-Experten) sichern ihre Daten vor möglichst allen Varianten von Datenverlust oder Datenzerstörung. Ursachen für einen solchen Verlust können Diebstahl, versehentliche Löschung oder auch absichtliche Änderungen sein. Glücklicherweise ist das Sichern von Daten einfacher, als Sie vielleicht denken. Wenn Sie sorgfältig planen und diese Backup-Pläne gut ausführen, ist es möglich, Ihre Daten auf allen Organisationsebenen zu sichern.

Folgende Datenelemente bzw. Datenstrukturen sollten Sie sichern:

- **Bootstrap-Daten:** werden zum Starten eines Computers verwendet. Dabei handelt es sich um ein kleines, spezielles Programm, das zuerst ausgeführt wird, wenn ein System eingeschaltet oder neu gestartet wird. Ohne einen gültigen Bootstrap ist ein System nicht funktionstüchtig.

- **Dateistruktur-Metadaten:** beschreiben, wo sich Dateien, Ordner, Bootstrap-Daten, das Betriebssystem, Treiber und Anwendungsprogramme befinden. In den Dateistruktur-Metadaten ist verzeichnet, welche Speicherblöcke auf der Festplatte mit Daten belegt und welche frei sind. Sie ordnen jedem Ordner und jeder Datei einem bestimmten Speicherort auf dem Laufwerk zu. Dieser Datentyp enthält außerdem Berechtigungs- und Zugriffslisten, die unbefugte Lese- oder Schreibvorgänge verhindern, indem diese Listen bei Zugriffen abgearbeitet werden. Die Summe aller Dateien, Ordner und Dateistruktur-Metadaten wird auch als Dateisystem bezeichnet.

  In einigen Systemen werden Änderungen an Datensätzen protokolliert und so eine Art „Überwachungspfad“ gespeichert. Diese Protokolle werden beispielsweise bei plötzlichen Unterbrechungen (z. B. durch einen Stromausfall) verwendet und dienen dann der Wiederherstellung des Dateisystems. Diese Metadaten sind also genauso wichtig wie die eigentlichen Dateien und Ordner – insbesondere, wenn Sie ein ganzes System wiederherstellen müssen.

- **Treiber-Binärdateien:** steuern Geräte, die Daten einlesen oder schreiben – egal ob von einem optischen Datenträger, einem Magnetband oder aus dem Netzwerk. Treiber gehören oft zum Betriebssystem (siehe nächsten Absatz) und müssen mit dem verwendeten System kompatibel sein. Wenn Sie Geräte kaufen, deren Treiber nicht zum Betriebssystem gehören, liegen diese der Verkaufsbox auf einem Datenträger bei oder können aus dem Internet heruntergeladen werden.
- **Betriebssystem:** Der Software-Code eines Betriebssystems wurde früher ebenfalls meist auf Datenträgern ausgeliefert. Viele Hersteller liefern das Betriebssystem (und Updates für dieses) aber auch direkt mit dem System aus und/oder bieten es per Download über das Internet an. Die Bedeutung von Datenträgern lässt hier zunehmend nach.

  Es ist wichtig, dass Sie auch nach dem Update eines Betriebssystems ein Backup desselben erstellen. Nur so ist Ihr System auch dann aktuell, wenn Sie später eine Wiederherstellung durchführen müssen. Wenn Sie keine aktuelles Backup des Systems haben, müssen Sie bei einer späteren Wiederherstellung alle zwischenzeitlichen Updates neu aufspielen, was ein fehleranfälliger und zeitraubender Prozess sein kann.

- **Konfigurationsdateien:** sind vielfältig. Neben einfachen Dateien, die vielleicht nur den Namen oder die Zeitzone eines Systems enthalten, gibt es auch komplexe Konfigurationsdateien wie die Windows-Registry (eine Art Datenbank mit Tausenden von

wichtigen Systeminformationen). Auch bei Kennwortdateien handelt es sich um eine Art von Konfigurationsdateien. Es gibt Programme oder Systeme, die beim Verlust eines Kennworts nicht wieder richtig hergestellt werden können Darüber hinaus verfügen viele Anwendungen über komplexe Konfigurationsdateien, die verschiedene, für das System spezifische Informationen speichern.

- **Anwendungsprogramme:** manche Unternehmen kaufen ihre Anwendungen von anderen Herstellern, andere entwickeln wiederum ihre eigenen Anwendungen. Für Unternehmen, die selbst Software entwickeln, kann der Verlust des dazugehörigen Quellcodes ein besonders tragischer Fall von Datenverlust sein. Grundsätzlich gilt: Daten zu besitzen, ist das eine – aber wenn auch die Anwendungsprogramme verloren gehen, mit denen diese Dateien normalerweise verwendet und bearbeitet werden, nützen die Daten an sich auch nichts mehr. Ein Verlust des Anwendungsprogramms kann sich daher manchmal genauso auswirken wie der Verlust der eigentlichen Datendateien. Daher sollten nicht nur Unternehmen ihre Anwendungen (oder sogar das ganze System) mit der gleichen Sorgfalt sichern, wie die eigentlichen Datendateien (Dokumente, Texte, Tabellen, Fotos, Videos etc.).
- **Datendateien:** sind Dateien, die mit entsprechenden Anwendungsprogrammen (beispielsweise Tabellenkalkulationen oder Textverarbeitungen) erstellt und bearbeitet werden. Es gibt Datendateien, die nur für bestimmte Programme spezifisch sind, während andere von unterschiedlichen Programmen bearbeitet werden können. Datendateien können klein oder groß sein, sich selten, nie oder schnell verändern, leicht auf andere Systeme übertragbar sein oder durch bestimmte Mechanismen an ein System gebunden sein. Auf Unternehmensservern liegen oft Hunderttausende oder sogar Millionen von Datendateien.
- **Datenbanken:** können als eine spezielle Variante von Datendateien angesehen werden. Um die wichtige Konsistenz von Datenbanken zu gewährleisten, sollten bei ihrer Sicherung besondere Überlegungen bzw. Maßnahmen vorgenommen werden. Sie sollten nicht davon ausgehen, dass ein einfacher Backup-Prozess auch alle Arten von Datenbanken problemlos sichern kann. Zumeist sind besondere Backup-Mechanismen bzw. -Programme notwendig.

Beliebige Daten, beliebige Geräte, beliebige Speicherorte, beliebige Umgebungen

Seit mehr als 30 Jahren gibt es die Möglichkeit, komplette Computer zu virtualisieren. Durch die Einführung eines sogenannten „Software-Hypervisors" von der Firma VMware sind die Möglichkeiten dieser Technik regelrecht explodiert. Seitdem sind viele weitere Hypervisoren erschienen und werden komplexe Virtualisierungsfunktionen durch spezielle Hardware leistungssteigernd unterstützt. Solche Hardware-Unterstützungen, Multi-Core-Prozessoren und stark gewachsene Daten- bzw. Arbeitsspeicher sind die Ursache, dass moderne virtuelle Systeme längst so leistungsfähig sind, wie die früher nur physische Computer oder sogar Großrechner. Zudem können die Arbeitslasten von physischen Maschinen in virtuelle Umgebungen migriert werden – und umgekehrt.

Aufgrund dieser rasanten Entwicklung ist es wichtig, beim Thema Backup auch virtuelle Maschinen zu berücksichtigen. Wenn Sie mit virtuellen Umgebungen arbeiten, sollten Sie auch eine Backup-Lösung wählen, die nicht nur physische Systeme, sondern auch virtuelle Umgebungen (mit den gängigen Hypervisoren) sichern und wiederherstellen kann. Werden virtuelle Systeme bei der Erstellung, Speicherung und Wiederherstellung von Backup-Archiven verwendet, können Arbeitslasten besser verteilen und sich von bestimmten Hardware-Anforderungen befreien. Die Möglichkeit, Betriebssysteme, Anwendungen und Daten zwischen physischen, virtuellen und Cloud-Umgebungen (mit einem Hypervisor) zu migrieren, stellt also einen echten Mehrwert dar. Erst ein Backup-Produkt, das mit beliebigen Daten, beliebigen Umgebungen, beliebigen Speicherorten und beliebigen Geräten funktioniert, gibt Ihnen die größtmögliche Flexibilität, das gesamte Spektrum aktueller und zukünftiger Computerleistungen zu nutzen.

Backups einfach, vollständig und sicher gestalten

Das allgemeine Mantra für Backups lautet: „Einfach, vollständig und sicher". In diesem Abschnitt werde ich die dahinterstehenden Konzepte näher erklären.

Das Prinzip der Einfachheit

Einfachheit ist ein sehr wichtiger Faktor, da diese Eigenschaft hilft, Fehler zu vermeiden.

Nehmen wir ein Beispiel: ein Unternehmen, welches eine komplexe, über Jahre entwickelte Backup-Lösungen einsetzt. Bei dieser kann es leicht passieren, dass bestimmte Produkte und Backup-Medien zueinander inkompatibel sind. Ohne genaue schriftliche Anleitungen (z. B. in Form von Checklisten) bei Backup- und Wiederherstellungsprozessen ist hier Ärger schon fast vorprogrammiert. Die Befolgung schlecht dokumentierter Anweisungen kann leicht bewirken (insbesondere unter Zeitdruck), dass Daten aus falschen Backups wiederhergestellt werden oder korrekte Daten mit fehlerhaften überschrieben werden.

Leicht bedienbare Benutzeroberflächen mit minimalem Einrichtungsaufwand und einer „Ein-Klick"-Wiederherstellung sind meist wichtiger und empfehlenswerter als klassische Checklisten und Pläne. Achten Sie also darauf, dass Sie die Benutzerfreundlichkeit berücksichtigen und ein einfaches, vollständiges und sicheres Backup-Produkt auswählen.

Vollständigkeit verstehen

Vollständigkeit bedeutet, sowohl über alle Daten zu verfügen, die für die Wiederherstellung eines Systems erforderlich sind – wie auch über die richtigen Werkzeuge und Prozesse. Wenn Ihre Backup-Software es beispielsweise ermöglicht, eine bootfähige CD oder DVD zu erstellen, können Sie mit dieser auch dann eine Wiederherstellung durchführen, wenn das eigentliche Betriebssystem nicht mehr starten kann. Falls Sie eine Backup-Software ohne diese Funktion verwenden, müssen Sie stattdessen das Betriebssystem neu installieren – oder zumindest alle Konfigurationen und Updates erneut durchführen. Das kann ein sehr langwieriger und fehleranfälliger Prozess sein.

Das Backup-Programm sollte außerdem in der Lage sein, Festplatten zu partitionieren und zu formatieren. Und insbesondere für den Fall, dass Sie ein System auf fabrikneuer Hardware wiederherstellen müssen. Da diese Aufgabe schwierig und fehleranfällig ist, sollte die Backup-Software Ihnen dabei helfen oder diese Prozesse ganz automatisch durchführen können.

Last but not least sollte der Backup-Software auch eine ausführliche Anleitung beiliegen (am besten gedruckt oder druckbar), damit Sie Backup- und Wiederherstellungsprozess möglichst fehlerfrei

durchführen können. Vergleichbar zu einem Flugkapitän, der eine Checkliste abarbeitet, um sein Flugzeug auch sicher starten und landen zu können.

Zusammenfassend bedeutet das: der Begriff „Vollständigkeit" bezieht sich auf die Daten, die Geräte, die Speicherorte und die Systemumgebung. Alles sollte möglichst vollständig vorliegen und/oder vollständig unterstützt werden.

Auf Sicherheit vertrauen

Sicherheit hat zwei Aspekte:

- **Zuverlässigkeit:** Backup-Daten müssen für eine Sicherung zuverlässig erfasst werden und fehlerfrei lesbar sein. Sollte das Backup noch von weiteren Daten abhängen, müssen auch diese verfügbar und lesbar sein. Die Backup-Software kann verschiedene Techniken zum sicheren Erfassen von Daten verwenden. Wenn diese Daten nicht gelesen werden können, kann auch das System nicht wiederhergestellt werden. Das Fehlen eines einzigen Datenelements kann im schlimmsten Fall dazu führen, dass ein komplettes System nicht wiederhergestellt werden kann.
- **Schutz:** Nachdem die Daten erfasst wurden, müssen sie vor Änderungen und Diebstahl geschützt werden. Wenn Ihr Backup-System nicht geschützt ist, können unbefugte Personen in das System eindringen, Daten stehlen und/oder das System beschädigen (ohne dass Sie es bemerken). Ein solches Szenario gilt es natürlich möglichst zu vermeiden.

Vorbeugung ist beim Thema Backup also besonders wichtig. Halten Sie Ihre Backup-Prozesse möglichst einfach und dokumentieren Sie Ihre Sicherungen gut. Dies beginnt schon im ersten Schritt, der ordnungsgemäßen Datenerfassung (siehe Kapitel 2). Denn wenn Sie die Daten falsch erfassen, können Sie die Hoffnung auf eine sichere Wiederherstellung gleich wieder fallen lassen.

Kapitel 2

Daten für ein Backup erfassen

In diesem Kapitel

- Image- und Datei-Backups verstehen
- Einen Backup-Plan erstellen
- Agenten verwenden (oder nicht)
- Backup-Produkte auswählen

Viele Anwender verstehen unter einem Backup leider nur, einfach ein paar wichtige Dateien auf einen separaten Datenträger (z. B. einen USB-Stick) zu kopieren. In Arbeitsrechnern, großen Systemen und Servern befinden sich aber mitunter sehr viele Dateien – und oft ändern sich die in ihnen enthaltenen Daten auch noch ständig. Ein systematisches Mittel zum Erfassen von Systemdaten, Anwendungen und Metadaten (sogar während Dateien geöffnet sind und geändert werden) ist obligatorisch, wenn Sie verloren gegangene oder beschädigte Daten sowie Anwendungen wiederherstellen möchten.

In diesem Kapitel werde ich Schritt für Schritt die wichtigsten Backup-Varianten sowie den notwendigen Umfang von Backups besprechen. Typische Backup-Situationen sollen Ihnen helfen, diese Grundlagen leichter in die Praxis zu übertragen.

Backup-Typen verstehen

Für systemnahe Programme sehen die meisten Speichergeräte (Bandgeräte einmal ausgenommen) wie Laufwerke aus. Das gilt auch für CD-/DVD-Geräte (unabhängig von möglichen Brennfunktionen). Die Hardware präsentiert dem Betriebssystem den verfügbaren Speicherplatz als eine Sequenz von Blöcken. Jeder Block ist dabei normalerweise les- und schreibbar. Die meisten dieser Blöcke nehmen normale Daten (in Form von Dateien) auf. Andere enthalten *Metadaten*, die Verzeichnisse, eine Auflistung belegter, freier oder beschädigter Blöcke, Bootstrap-Daten, Partitionsinformationen und ähnliches enthalten.

Der von den Metadaten belegte Speicherplatz steht Ihnen nicht als freier Speicherplatz für Ihre Daten zur Verfügung. Deshalb ist der verfügbare freie Speicherplatz, den Sie auf einer Festplatte sehen, geringer als die vom Anbieter angegebene Bruttokapazität.

Diese Art der Datenorganisation und die Unterscheidung zwischen Daten und Metadaten ist wichtig, wenn es um die zwei wesentlichen Verfahren geht, mit denen die Daten eines Laufwerk für ein Backup erfasst werden. Und zwar unterscheidet man dabei zwischen den komplexeren Image-Backups und den einfacheren Datei-Backups. Beide Verfahren werden in den folgenden Abschnitten noch ausführlich erläutert.

Obwohl Ihnen beide Verfahren ermöglichen, später nach bestimmten Dateien und Daten zu suchen, ist das Image-Backup dem Datei-Backup übergeordnet, da es neben den eigentlichen Daten zusätzlich auch noch System-Metadaten enthält.

Datei-Backups

Der ursprüngliche Backup-Typ war ein *Datei-Backup*, das immer noch sehr beliebt ist. Bei einem Datei-Backup werden bestimmte oder alle Dateien und Ordner auf ein Backup-Medium kopiert. Der Prozess entspricht im Prinzip dem manuellen Kopieren persönlicher Dateien auf einen USB-Stick oder in ein Netzwerkverzeichnis, nur dass er von einer Backup-Software natürlich mit zusätzlichen „Raffinessen“ funktionell aufgewertet wird und automatisiert werden kann.

Da Dateisysteme überwachen, ob und wann eine Datei erstellt sowie geändert wird, kann man ein Datei-Backup auch so konfigurieren, dass nur solche Dateien und Ordner kopiert werden, die seit der vorherigen Sicherung geändert wurden. Der eigentliche Kopierprozess scheint für ein Backup-Programm an sich eine leichte Aufgabe, da das Betriebssystem dafür alle erforderlichen Funktionen bereitstellt. Jedoch benötigt ein Backup-Programm schon einen gewissen Mehraufwand, da es sich bei der Sicherung um Folgendes kümmern muss:

1. **Die Blöcke suchen, in denen sich die betreffenden Ordner befinden.**
2. **Diese Ordner lesen.**
3. **Nach den Namen der zu sichernden Dateien suchen.**
4. **Die genaue Speicherposition (Blöcke) dieser Dateien ermitteln.**
5. **Diese Blöcke lesen und kopieren.**

Dieser Prozess kann (je nach Geschwindigkeit des Laufwerks und der Datenmenge) einige Zeit in Anspruch nehmen. Wenn das System zu diesem Zeitpunkt noch mit weiteren Aufgaben beschäftigt ist, kann der Backup-Prozess durchaus die Systemressourcen spürbar beanspruchen. Dies hängt allerdings von vielen Faktoren ab, insbesondere der Leistungsfähigkeit des verwendeten Systems.

Image-Backups

Ein *Image-Backup* umgeht den Aufwand der Dateisuche, indem es keine Dateien, sondern stattdessen die reinen Datenblöcke eines Laufwerks kopiert. Als Ergebnis wird ein Art „Abbild" (die hier passende Übersetzung des englischen Wortes „Image") der Festplatte erstellt. Image-Backup-Software wurde von Menschen entworfen, die ein tiefes Verständnis darüber haben, wie genau Daten auf Festplatten organisiert sind. Auch bei einem Image-Backup kann die Software ermitteln, welche Datenblöcke seit dem letzten Backup geändert wurden und (sofern gewünscht) ausschließlich diese Blöcke kopieren. Wenn z. B. bei einer 2 GB großen Datei seit der letzten Sicherung nur eine kleine Änderung vorgenommen wurde, muss bei einem Datei-Backup, das auf einem vorherigen Backup aufbaut und nur geänderte Daten sichern soll, dennoch die gesamte Datei mir ihren 2 GB kopieren werden. Bei einem Image-Backup (das ebenfalls auf einem vorherigen Backup aufbaut), muss dagegen im Idealfall nur der eine geänderte Sektor gesichert werden. In einer solchen Konstellation kann ein Image-Backup daher deutlich schneller (und im Resultat kleiner) als ein Datei-Backup sein.

Eine moderne, schnelle Backup-Software kann Daten nicht nur als Dateien sichern, sondern (auf Wunsch) auch über die Datenblöcke, die von der Datei auf dem Laufwerk belegt werden. Auf Wunsch kann sie dabei außerdem fehlerhafte, temporär belegte, ungenutzte und unveränderte Blöcke sichern – und so die Größe des resultierende Laufwerk-Image klein halten. Natürlich ist es auch möglich, nicht erwünschte/benötigte Dateien vom Backup auszuschließen.

Trotz Organisation in Datenblöcken können auch bei Image-Backups einzelne Dateien gesucht und wiederhergestellt werden. Außerdem können Image-Backups wie (virtuelle) Festplatten ins System eingebunden („gemountet") werden. Auf diese Weise kann man leicht auf bestimmte Dateien zugreifen oder auch Dateien aus unterschiedlichen Backup-Zeitpunkten überprüfen und auf mögliche Veränderungen vergleichen.

Beide Backup-Typen (Image- und Datei-Backups) können vollständig, differentiell oder inkrementell erstellt werden. Ich werde diese drei wichtigen Backup-Typen im nächsten Abschnitt erläutern.

Images werden oft auch mit dem englischen Wort *Snapshots* bezeichnet, was wörtlich „Schnappschuss“ bedeutet. Dieser Begriff hat in Bezug auf Backups jedoch zwei unterschiedliche Bedeutungen, daher ist für den hier besprochenen Backup-Typ der Begriff *Image-Backup* dem Begriff *Snapshot-Backup* vorzuziehen. Ich behandle Snapshots später im Abschnitt „Einen Snapshot erstellen“.

Ein Backup nach Plan ausführen

Ein Backup-Plan beschreibt den genauen Ablauf eines Backups, also Backup-Quelle/-Ziel, Datenumfang, Zeitpunkt und ähnliche Parameter. In diesem Abschnitt behandele ich einige grundlegende Entscheidungen, die Sie bei Erstellung eines Backup-Plans treffen sollten.

Die Wahl zwischen einem vollständigen, differentiellen oder inkrementellen Backup

In Bezug auf den zeitlichen Prozess, mit dem Backups nacheinander in einer Kette erstellt werden können, lassen sich drei Typen unterscheiden:

- **Vollständiges Backup:** Das erste Backup (innerhalb einer Backup-Kette), bei dem alle gewünschten Daten erfasst werden. Ein vollständiges Backup wird oft auch kurz einfach nur *Voll-Backup* genannt.

  Der Vorteil (im Vergleich zu den nachfolgenden Typen) eines vollständigen Backups ist, dass es in sich abgeschlossen ist. Sein Nachteil ist, dass es viel Speicherplatz beansprucht, der Backup-Prozess viel Zeit benötigt und seine Daten sich trotz des hohen Speicherbedarfs unter Umständen wenig zu einem vorherigen vollständigen Backup unterscheiden. Erstellt man beispielsweise häufiger Sicherungen des Betriebssystems, kann die sich anhäufende Summe vieler Voll-Backups sehr groß werden, sofern man gerne mehrere Versionen seiner Sicherungen aufbewahrt.

- **Differentielles Backup:** Eine Art Teil-Backup, das nur die Unterschiede zwischen dem aktuellen Status und dem letzten vollständigen Backup in derselben Backup-Kette erfasst. Wenn Daten aus einem differentiellen Backup wiederhergestellt werden, müssen sowohl das letzte Voll-Backup als auch das betreffende differentielle Backup gültig bzw. intakt sein. In jedem Fall müssen bei einer Wiederherstellung hier immer zwei Backup-Versionen (das Voll-Backup und das differentielle) eingelesen werden.

Der Vorteil eines differentiellen Backups ist, dass es meist bedeutend schneller als ein vollständiges Backup ist. Sein wesentlicher Nachteil tritt im Vergleich zum nächsten Backup-Typ auf: differentielle Backups sind meistens größer als inkrementelle.

- **Inkrementelles Backup:** Ein weiteres Teil-Backup, das (zuerst einmal ähnlich wie beim differentiellen Backup) nur die Unterschiede zwischen dem aktuellen Status und der letzten Backup-Version in derselben Backup-Kette sichert. Anders als differentielle Backups, die immer nur das letzte Voll-Backup zum Abgleich/Vergleich heranziehen können, kann ein inkrementelles Backup aber auch auf einem zuletzt erstellten differentiellen oder inkrementellen Backup aufbauen.

  Der Vorteil eines inkrementellen gegenüber einem differentiellem Backup ist, dass es kleiner und schneller sein kann (letztendlich immer auch abhängig von der Art der vorliegenden Daten). Sein Nachteil ist, dass bei einer Wiederherstellung alle vorherigen Backups in der Backup-Kette benötigt werden – und die betreffenden Daten in diesen lesbar und gültig vorliegen müssen. Betrachtet man einen angestrebten Wiederherstellungszeitpunkt (Recovery Point Objective, siehe nächsten Abschnitt) wird also das anfängliche Voll-Backup benötigt – und dann alle bis zu diesem Wiederherstellungszeitpunkt erstellten Teil-Backups. Die Wiederherstellung eines inkrementellen Backups kann also unter Umständen recht zeitaufwendig und komplex werden.

Die meisten modernen Backup-Programme verfügen über eine Funktion, die „Konsolidierung“ genannt wird. Bei dieser wird versucht, nicht mehr benötigte oder redundante Daten in größeren Backup-Ketten „zusammenzudampfen“, sodass der benötigte Speicherplatz reduziert wird. Inkrementelle Backups können unabhängig von der ursprünglichen Quelle (quasi „offline“) konsolidiert werden, indem z. B. mehrere inkrementelle Backups zu einem kompakten differentiellen zusammengeschrieben werden. Das kann sich positiv auf die Zuverlässigkeit und Wiederherstellungszeit auswirken. Bei einem sogenannten *umgekehrt-inkrementellen Backup* erfolgt die Konsolidierung sogar piffigerweise schon direkt während der Backup-Erfassung. Eine weitere Abwandlung wird *immer-inkrementell* genannt, hat aber je nach Anbieter unterschiedliche Bedeutungen, sodass wir sie hier nicht näher erläutern.

Bei den meisten Datenbeständen beträgt die Größe des täglichen Backups (und damit die Größe der inkrementellen Backup-Dateien) – 3 bis 5 % eines vollständigen Backups. Diese Zahl variiert jedoch stark (je nach Typ der Daten). Inkrementelle Backups werden außerdem bei umfassenden Änderungen am Datenbestand sehr schnell sehr groß – beispielsweise beim Upgrade von Anwendungsprogrammen oder der Umorganisation eines Datenbestandes, wie er beispielsweise auch schon durch die Defragmentierung einer Festplatte auftreten kann. Wenn Sie wichtige Updates oder Upgrades planen, sollten Sie die betreffenden Daten in der Regel vor und nach diesen Änderungen in Form eines vollständigen Backups sichern. Inkrementelle Backups empfehlen sich dagegen, wenn Sie häufig kleinere Änderungen an einem Datenbestand oder einem System vornehmen.

Den RPO festlegen

Ein *angestrebter Wiederherstellungszeitpunkt (Recovery Point Objective, RPO)* definiert, wie oft bzw. mit welchem Intervall Backups erfolgen sollen. Ein *Backup-Fenster* bezeichnet die Zeitspanne, in der ein System für ein Backup angehalten werden darf. Ziel ist es, solche Backup-Fenster möglichst zu vermeiden. Dazu wurden Techniken entwickelt, bei denen ein aktives, laufendes System – inklusive der im Betrieb gerade geänderten Daten – gesichert werden kann. ohne dass das System dabei pausiert oder sogar ausgeschaltet werden muss. Backup-Fenster und RPO stehen schnell in einem Konflikt, insbesondere wenn häufige Wiederherstellungspunkte gewünscht sind und jeder Backup-Prozess das System ausbremst.

Der RPO legt also das Intervall fast, wie häufig die einzelnen Wiederherstellungspunkte erstellt werden sollen. Wenn das RPO-Intervall beispielsweise 30 Minuten beträgt, bedeutet dies, dass alle 30 Minuten ein Wiederherstellungspunkt gesetzt wird. Das Backup-Fenster definiert, wie viel Zeit für den Backup-Prozess zur Verfügung steht. Bei einem 30 minütigen RPO beispielsweise sollte das Backup-Fenster kürzer als 30 Minuten sein. Und wenn die Backups nur zwischen Mitternacht und 02:00 Uhr durchgeführt werden können, darf der RPO nicht kürzer als ein Tag sein, denn: würde das Backup um 02:00 Uhr abgeschlossen, wäre der letzte Wiederherstellungspunkt am Vortag um 02:00 Uhr.

Es stehen viele Methoden zur Verfügung, um Backup-Fenster zu verkürzen und häufigere Wiederherstellungspunkte zuzulassen. Sie alle erfordern jedoch zusätzliche Systemressourcen. Ein System muss über ausreichend Leistung verfügen, um seine eigentliche Arbeit und gleichzeitig (innerhalb eines Backup-Fensters) auch ein Backup auszuführen. Eine gute Backup-Software beansprucht möglichst wenig

eigene Ressourcen und kann diese zudem an die Auslastung des zu sichernden Systems anpassen. Dadurch kann es zwar länger dauern, bis ein Backup abgeschlossen ist – gleichzeitig wird das System aber weniger eingeschänkt.

Fakten und Beurteilungen im Hinblick auf den RPO

RPOs richtig festzulegen, ist eine Frage, bei der man etliche *Fakten* und Beurteilungen gegeneinander abwägen muss. Solche Fakten sind beispielsweise die Kosten für Ausfallszeiten – aber auch für die Umsetzung der RPOs. Bei den *Beurteilungen* geht es darum, mögliche Risiken und Schäden (auch immaterielle, wie den Verlust eines guten Rufes) abzuwägen. Wenn Sie sich beispielsweise in Werbe- und Marketingkampagnen eher als Low-Cost-Anbieter positionieren, könnten Sie erwägen, beim Backup zu sparen. Wenn Sie jedoch explizit damit werben, keine Ausfallzeiten zu haben und keine Daten zu verlieren, kann auch eine kurze Störung oder der Verlust eines wichtigen Datensatzes (z. B. Bestelldaten in einem Online-Shop) Ihr Geschäft und Ihren Ruf schädigen.

Wenn Sie tatsächlich gewährleisten wollten, von jedem einzelnen Wiederherstellungspunkt später auch wirklich eine komplette Wiederherstellung durchführen zu können, müssten Sie eine sehr große Zahl von Backup-Dateien aufbewahren. Besser ist es, ein flexibles, verschiebbares RPO-Intervall festzulegen, indem Sie die Archive älterer Wiederherstellungspunkte löschen. Beispiel: Bei geschäftskritischen Arbeitslasten setzen Sie den RPO für die jeweils letzten 24 Stunden auf ein 5 Minuten-Intervall. Dieses Intervall vergrößeren Sie dann, je älter die Daten sind. Z. B. auf eine Stunde für die vergangenen Tage, auf täglich für den vergangenen Monat. Von den noch älteren Daten bewahren Sie nur ein monatliches Backup dauerhaft auf. Dies lässt sich natürlich anpassen. Weniger wichtige oder seltener geänderte Daten können auch entsprechend seltener gesichert werden – und die älteren Archive schneller gelöscht werden.

Kosten, Vorteile und Risiken abwägen

Kosten, Vorteile und Risiken sorgsam und richtig abzuwägen, kann schwierig sein. Ein solcher Abwägungsprozess hilft Ihnen aber, herauszufinden, welchen RPO (also welches Intervall) Sie einrichten sollten. Extremstandpunkte – etwa, dass man auf keinen Fall jemals irgendwelche Daten verlieren möchte – relativieren sich schnell, wenn man erkennt, welche Kosten dies verursachen kann. Backups sind auch nicht dazu gedacht, als alleiniges Werkzeug zu garantieren, dass ein Betrieb absolut fehler- und ausfallsfrei läuft. Es ist ein Instrumentarium, das durch weitere (z. B. redundante Systeme) ergänzt werden sollte.

Eine weitere Erwägung ist der benötigte Zeitrahmen für die Erstellung eines Backups. Ein Backup-Prozess muss innerhalb eines ihm zugedachten Backup-Fenster auch abgeschlossen werden können. Der zugewiesene Zeitrahmen muss dabei auch mit den vorgegebenen minimalen Ausfallszeiten abgestimmt werden. Wenn Sie eine maximale Ausfallszeit 15 anvisieren, das Backup-Fenster aber größer ist, kann dies nicht funktionieren. Sie haben verschiedene Möglichkeiten, Backup-Fenster so zu reduzieren, dass der RPO möglichst wenig beeinträchtigt wird. Die einfachste Möglichkeit, Backup-Fenster zu reduzieren, ist die Verwendung eines Snapshots (siehe nächsten Abschnitt). Dieser Prozess birgt jedoch auch Risiken.

Einen Snapshot erstellen

Eine Möglichkeit, Backups zu beschleunigen, besteht darin, die Menge der kopierten Daten zu reduzieren. Die gängige Methode funktioniert folgendermaßen: das betreffende System wird kurz angehalten, um einen Snapshot (eine Kopie der Metadaten) zu erstellen. Dieser Vorgang dauert nur einen Bruchteil der Zeit, die zum Kopieren der eigentlichen Daten benötigt wird. Die Daten selbst werden im anschließenden Backup erfasst. Die Metadaten im Snapshot werden dazu verwendet, die Dateien für das Backup schneller zu finden. Sollten die Daten nun während des Betriebs geändert werden, so werden auch die ursprünglichen Metadaten aktualisiert – jedoch nicht die Metadaten in der Snapshot-Kopie. Die Konsequenz ist, dass im Backup keine Daten enthalten sind, die nach der Aufnahme des Snapshots geändert oder hinzugefügt wurden. Ein Snapshot verweist auf den Großteil der Daten und enthält nur dann tatsächliche Daten, wenn diese geändert wurden. Eine Alternative bestünde darin, das System anzuhalten und dabei alle Daten (vollständiges Backup) oder die Daten, die seit dem letzten Backup geändert wurden (differentielles oder inkrementelles Backup), aufzuzeichnen. Diese Alternative ist zwar sicherer, dauert aber viel länger und unterbricht den Betrieb, da laufende Anwendungen bis zum Abschluss des Backups angehalten werden.

Snapshots verkürzen Backup-Fenster erheblich. Sie sind insbesondere dann nützlich, wenn Daten oft aktualisiert werden, da ein System von einem Snapshot einfach wiederhergestellt werden kann. Snapshots sind insbesondere bei Storage Area Networks (SANs) wichtig, da SANs Ressourcen sind, die von vielen Komponenten in einem System gemeinsam genutzt werden. Werden Sie auch nur für ein paar Sekunden angehalten, können sie dennoch einen Großteil des Systems unterbrechen. Snapshots sind jedoch nur bei kurzfristiger Verwendung sicher. Zudem kann das

Verwalten von Snapshot-Löschvorgängen erhebliche Ressourcen in Anspruch nehmen.

Ein Snapshot ist keine vollständige Kopie von Daten. Wenn eine Festplatte als Backup-Quelle dient und bei Backup-Erstellung beschädigt war, ist auch der Snapshot beschädigt. Snapshots mögen auf kurze Sicht sicher sein, ein Ersatz für Backups sind sie aber nicht.

Es gibt spezielle Techniken, die helfen, das Backup-Fenster eines Snapshot-Prozesses zu verkürzen. VMware verwendet ein solches Verfahren, Changed Block Tracking (CBT) genannt, mit der die Erfassungszeit der Backup-Software verkürzt werden kann. Der Volume Shadow Copy Service (VSS) von Microsoft ist eine weitere derartige Technik. Zu sichernde Anwendungen wie auch die Backup-Software müssen mit diesen Technologien funktionieren bzw. kompatibel sein, um vollständige und korrekte Backups erzeugen zu können.

Backups mit oder ohne Agenten erstellen

Backup-Programme können auf zwei Arten auf die Daten eines Systems zugreifen:

- Mit einem Agenten: Ein kleines Backup-Programm, ein Agent, wird auf betreffenden physischen Computern und virtuellen Maschinen (VMs) installiert.
- Ohne einen Agenten: In virtuellen und Cloud-Umgebungen kann die Zahl der VMs ziemlich groß werden, sodass auch agentenlose Backups eine Rolle spielen.

Tatsächlich verwenden auch agentenlose Backups bestimmte Agenten, jedoch in geringer Anzahl, um den Prozess leichter zu verwalten. In der Regel wird nur ein Agent auf jedem virtuellen Host installiert (der üblicherweise auch als VM läuft). Dieser Agent kann mit dem Host kommunizieren und nun auch jede VM auf diesem Host sichern. Die meisten Hosts verfügen über mehrere Hosts – und da VMs zwischen Hosts migriert werden können, müssen die Backup- und Erfassungssysteme jederzeit erkennen können, wo sich jede einzelne VM befindet.

Mit agentenlosen Backups lässt es sich gut arbeiten. In besonderen Fällen, in denen der Host/Hypervisor nicht alle mit der VM verbundenen Objekte sichern kann, sollten Sie einen Agenten installieren, um diese Maschine direkt zu sichern. In den meisten Fällen kümmert sich jedoch der Agent des Hosts um alles.

Sie müssen sicherstellen, dass Sie die richtige Anzahl von Agenten installieren, diese regelmäßig aktualisieren und (sofern erforderlich) eine gültige Lizenzdatenbank besitzen.

Überlegungen zu Backup-Produkten

Früher wurden Image-Backups von einer darauf spezialisierten Anwendung erstellt – und Datei-Backups von einer anderen. Heute zeichnet sich eine gute Backup-Software dadurch aus, dass sie mit beiden Backup-Typen umgehen kann. Solche Backup-Produkte können vollständige, differentielle und inkrementelle Backups (weiter oben in diesem Kapitel erörtert) sowie Snapshots erstellen, um Backup-Fenster zu verkürzen (ebenfalls weiter oben erörtert).

Einige Netzlaufwerke sowie einige SAN- und NAS-Speichersysteme können kein Image-Backup ausführen, da die Backup-Agenten über keinen steuerbaren Zugriff auf die Metadaten verfügen. Als Faustregel gilt: erstellen Sie wann immer möglich Image-Backups und sichern Sie Daten nur dann auf Dateiebene, wenn Sie einen guten Grund dafür haben (beispielsweise, weil ein Image-Backup technisch nicht möglich ist).

Eine leistungsfähige Backup-Anwendungen kann ein neues System komplett aus einem Image wiederherstellen. Dabei sind möglicherweise einige Anpassungen notwendig, insbesondere wenn sich die Hardware des alten (gesicherten) Systems und die des neuen (wiederherzustellenden) Systems unterscheiden. So müssen beispielsweise unterschiedliche Festplattengrößen angepasst werden, fehlende Treiber für Geräte-Controller installiert werden oder der Bootstrap des Betriebssystems angepasst werden. Wenn eine Backup-Software dazu in der Lage ist, kann sie damit auch zur Migration verwendet werden, beispielsweise um physische auf virtuelle Systeme umzustellen (oder umgekehrt).

Schnelle Backup-Programme erfassen nur Datenblöcken, die verwendet werden. Fehlerhafte und/oder ungenutzte Datenblöcke werden nicht mitgesichert.

Bare-Metal-Restore

Den Begriff *Bare-Metal* verwendet man für Systeme, auf denen noch keine Software (insbesondere kein Betriebssystem) installiert ist. Im Deutschen ist auch der Begriff „fabrikneu“ üblich. Unter Bare-Metal-Restore versteht man die Wiederherstellung eines (Betriebs)Systems auf solch fabrikneuer Hardware. Da Datei-Backups im Gegensatz zu Image-Backups keine System-Metadaten

und keinen Bootstrap enthalten, kann man mit ihnen keine Bare-Metal-Wiederherstellung durchführen. Der große Vorteil von Image-Backups besteht darin, dass man mit ihnen nicht nur einzelne Dateien, sondern auch Bare-Metal-Systeme wiederherstellen kann. Das gilt auch dann, wenn das ursprüngliche System, auf dem das Backup erstellt wurde, eine andere Hardware als das neue Zielsystem verwendet (hat). Im Idealfall kann eine solche Backup-Software also auch ein physisches Image (= das Image eines physischen Computersystems) in ein virtuelles Image konvertierten bzw. auf einem virtuellen System wiederherstellen – und umgekehrt. Ein solches virtuelles Image sollte sich dann auch in ein gängiges Virtualisierungssystem exportieren lassen. Informieren Sie sich bei Bedarf beim Anbieter der Backup-Software, über ein universelles Backup-Format verwendet wird, das gleichermaßen auf physischen wie auch virtuellen Maschinen (VMs) wiederhergestellt werden kann.

Single-Pass-Backup

Der Begriff *Single-Pass-Backup* bedeutet, dass nur ein Durchgang erforderlich ist, um die Daten zu erfassen und das Backup zu speichern. Auch die entsprechende Wiederherstellung der Daten erfolgt normalerweise in einem Schritt. Single-Pass-Backups sind schneller als Multi-Pass-Backups und können daher häufigere Wiederherstellungspunkte und ein kürzeres Backup-Fenster bieten.

Wenn Image- und Anwendungs-Backups in demselben Produkt kombiniert sind, können alle für eine vollständige Wiederherstellung erforderlichen Daten in einem einzigen Durchgang erfasst werden. Wenn Sie jedoch je ein Produkt für Image-Backups, eines für Datei-Backups und eines für Anwendungs-Backups verwenden, müssen Sie immer noch drei Backup-Durchgänge vornehmen (selbst wenn es sich bei den Produkten um Single-Pass-Produkte handelt). Die Daten werden für jedes Produkt in separaten Archiven gespeichert und getrennt verwaltet, was für zusätzliche Komplexität sorgt und das Risiko einer fehlerhaften Wiederherstellung erhöht.

Anforderungen an eine gute Datenerfassung

Bei der Festlegung Ihrer Datenerfassungsanforderungen sollten Sie Folgendes berücksichtigen:

- RPO nach Subsystem und Anwendung
- Backup-Fenster oder Dauer der Ausfallzeit, die für das Backup akzeptabel ist
- Backup-Typ (Image, Datei oder beide)
- Welche Anwendungen werden abgedeckt?
- Wie viele Backup-Prozesse können sicher verwaltet werden?

Falls Ihre Image-, physischen, virtuellen, Cloud-, Datenbank-, E-Mail- und Benutzer-Backups unterschiedliche Programme und Verwaltungsprozesse erfordern, werden die resultierenden Backup-Dateien vermutlich nicht kompatibel sein. Eine solche Vielfalt und Komplexität kann die Sicherheit Ihrer Daten bedrohen. Neue Innovationen im Computerbereich (bei Architekturen und Hardware) bringen zwar Vorteile mit sich, können es aber auch erschweren, Daten und Anwendungen auf neue Systeme zu migrieren. Wenn Sie ein einzelnes Backup-System verwenden können, das mit all diesen Aspekten (Architekturen, Hardware, Betriebssystemen, Anwendungen, Datentypen, physischen und virtuellen Maschinen und allen Hypervisoren) umgehen kann, müssen Sie sich nicht auf bestimmte Verfahren und Systeme festlegen. Bei der Wahl eines Backup-Systems sollte außerdem darauf geachtet werden, dass es möglichst lange verfügbar ist (eine hohe Lebensdauer auf dem Markt hat) und mit beliebigen Daten und Verarbeitungstypen funktioniert.

Kapitel 3

Backups sicher speichern

In diesem Kapitel

- Eine Speicherrichtlinie festlegen
- Software, Hardware und Standorte auswählen
- Komprimierung und Deduplizierung verstehen
- Speicherkosten schätzen

Eine klassische Maxime für Backups ist die sogenannte 3-2-1-Regel: Bewahren Sie drei Kopien Ihrer Daten auf zwei verschiedenen Medientypen auf – und eine Kopie sollte zudem an einem separaten (externen) Standort gespeichert werden.

Diese Medientypen waren früher insbesondere Bandgeräte (bei Unternehmen), optische Datenträger (bei Privatanwendern) und natürlich Festplatten. In Unternehmen werden Bandgeräte zunehmend durch die Cloud ersetzt oder ergänzt. Cloud-Speicher werden auch deswegen immer relevanter, weil sie sowohl die Forderung nach einem anderen Medientypen wie auch nach einem separaten Speicherort erfüllen. Die Kosten für die Cloud sind bei kleinen Datenmengen insbesondere dann niedrig, wenn Sie sich durch die Speicherung in der Cloud auch die Kosten für eine zusätzliche lokale Kopie sparen. Bei kleinen Datenmengen verlangen Cloud-Backups keine großen Investitionen.

In diesem Kapitel wird nun die sichere Speicherung Ihrer Backup-Daten erörtert.

Eine Backup-Richtlinie festlegen

Ihr Unternehmen verfügt möglicherweise bereits über eine Backup-Richtlinie, die auf bestehenden Systemen und Methoden basiert. Aber wenn Sie in Erwägung ziehen, neue Technologien hinzuzufügen, müssen Sie Ihre alten Methoden gegebenenfalls aktualisieren. Dieser Abschnitt gibt Ihnen einige Tipps zur Festlegung einer effektiven Backup-Richtlinie und eines Backup-Plans.

Backup-Plan

Ein Backup-Plan legt fest, welche Daten zu welcher Zeit gesichert werden sollen. Er kann so einfach oder komplex sein, wie Sie es für richtig halten:

- Ein einfacher Backup-Plan kann darin bestehen, täglich um Mitternacht ein vollständiges Image-Backup auszuführen.
- Ein komplexer Backup-Plan könnte ein wöchentliches Voll-Backup, ein allnächtliches differenzielles Backup und ein inkrementelles Backup alle vier Stunden umfassen. Die Backups auf zwei Maschinen (A und B) könnten um 22:00 Uhr starten, mit einer zufälligen Verzögerung von bis zu zwei Stunden; die Backups auf zwei weiteren Maschinen (C und D) könnten um Mitternacht starten, mit einer zufälligen Verzögerung von zwei Stunden; und die Backups auf nochmals zwei weiteren Maschinen (E und F) könnten um 02:00 Uhr starten, ebenfalls mit einer zufälligen Verzögerung von zwei Stunden. (Siehe Kapitel 2 für weitere Informationen zu vollständigen, differenziellen und inkrementellen Backups.)
- Ein noch komplexerer Plan könnte vorsehen, ein System-Image wöchentlich, ein Windows-Exchange-System fortlaufend, ein Microsoft-SharePoint-System jede Nacht, vorhandene Benutzerdateien alle zwei Tage (nach zufälligem Zeitplan), Systemkonfigurationsdaten wöchentlich, virtuelle Hosts wöchentlich und die Daten in einem Microsoft Active Directory alle acht Stunden zu sichern.

Es gibt zudem viele optionale Parameter – beispielsweise Bandbreitenbegrenzungen, die Frage, ob (zum Stromsparen) heruntergefahrene Systeme zum Backup aufgeweckt werden sollen und welche Fehlerereignisse protokolliert werden sollen. Letzteres kann nützlich sein, um Gegenmaßnahmen durchzuführen. Sie können beispielsweise ein Notfall-Backup starten lassen, wenn im Windows-Protokoll ein Festplattenfehler aufgezeichnet wird.

Ein gute Backup-Software lässt Ihnen bei der Erstellung eines Backup-Plans einen großen Spielraum. Ich empfehle die Verwendung eines Backup-Produkts, das eine umfangreiche Einstellung des Backup-Plans mit vielen Zusatzoptionen erlaubt. Wenn Sie beispielsweise Image-Backups erstellen wollen, wäre es auch nützlich, wenn diese Image-Backups in virtuelle Maschinen (VMs) konvertiert werden können, um diese so in einer virtuellen Umgebung starten zu können (siehe Infobox „Virtuell werden“ weiter unten im Kapitel.)

Aufbewahrungsrichtlinie

Ein wichtiger Bestandteil eines Backup-Plans ist die *Aufbewahrungsrichtlinie*. Sofern Sie nicht über sehr viel Speicherplatz für Backups

verfügen, müssen Sie irgendwann aus Platzgründen Wiederherstellungspunkte löschen. Die Aufbewahrungsrichtlinie legt fest, nach welchen Kriterien die Wiederherstellungspunkte aufbewahrt bzw. gelöscht werden sollen.

Bei der einfachsten Form einer Aufbewahrungsrichtlinie wird der Speicherplatz überwacht. Wird eine bestimmte Menge freien Speicherplatzes unterschritten, werden automatisch ältere Backups gelöscht. Die Entscheidung, nach welchen Kriterien welche Backups genau dann gelöscht werden sollen, kann jedoch schwierig sein. In den folgenden Abschnitten erörtere ich zwei gängige Arten von Aufbewahrungsrichtlinien, die ganz einfache Regeln (wie etwa, immer nur die allerältesten Wiederherstellungspunkte zu löschen) übersteigen. Die Verwendung einer so einfachen Regel ist keine gute Empfehlung. Es kann zu leicht passieren, dass auch auf ältere Backups zurückgreifen müssen, weil es sich erst spät herausstellt, dass Sie schon seit Monaten oder Jahren ein Problem in Ihrem System bzw. Datenbestand haben. Schauen wir uns daher zwei gängige komplexere Aufbewahrungsrichtlinien an.

GVS

Angenommen, Sie erstellen jeden Tag ein Backup. Am Ende einer Woche haben Sie sieben Backups und der Speicherplatz wird knapp. Also nehmen Sie eines der täglichen Backups, benennen es in ein wöchentliches Backup um und beginnen wieder mit den täglichen Backups. Am Ende der zweiten Woche nehmen Sie das letzte der täglichen Backups, benennen es in ein wöchentliches Backup um und fahren mit den täglichen Backups fort. Nach einer gewissen Zeit verfügen Sie über die täglichen Backups einer Woche sowie über etliche wöchentliche Backups. Der Speicherplatz wird jedoch weiterhin knapp, sodass Sie alle vier Wochen das wöchentliche Backup in ein monatliches Backup umbenennen und die wöchentlichen Backups wiederverwenden.

Dieser Richtlinientyp wird *Großvater-Vater-Sohn (GVS)* genannt. Dabei steht der Begriff „Sohn“ für die täglichen Backups, der „Vater“ für die wöchentlichen Backups und der „Großvater“ für die die monatlichen Backups.

Wenn Sie diese Richtlinie lange genug befolgen, ist jedoch auch hier irgendwann kein Speicherplatz mehr verfügbar und Sie müssen etwas löschen. Was löschen Sie? Falls Sie sich nicht entscheiden können, ziehen Sie die nächste Richtlinie in Betracht.

TVH

Der von mir empfohlene Aufbewahrungsplan wird „Türme von Hanoi“ (TVH) genannt. Ich möchte an dieser Stelle nicht zu sehr ins Detail gehen (die Einzelheiten sind zu Komplex, um hier im genau erörtert zu werden), aber lassen Sie mich das Prinzip grob umreißen. Ursprünglich handelt es sich eigentlich um ein Spiel bzw.

eine Art Puzzle, bei dem ein Turm aus Scheiben aufgebaut wird, die nach einem bestimmten Muster aufeinander gelegt bzw. verschoben werden dürfen. Die Spielregel lautet, dass immer nur eine Scheibe bewegt werden darf und und keine Scheibe auf einer kleineren liegen darf. Für den Computerbereich ist nun relevant, dass sich die übliche Lösungssequenz für dieses Puzzle auch als binäres Muster darstellen lässt – und bei Backups als Konzept für einen sehr effizienten Aufbewahrungsplan genutzt werden kann. Wenn Sie diesen TVH-Aufbewahrungsplan auf Backups anwenden, wird Ihr Speicherplatz effizient verwaltet und Sie können zudem Backups auch auf verschiedenen Medien speichern. Die Verwendung mehrerer Medien ist eine wichtige Schutzmaßnahme! Würden Sie nämlich all Ihre Backups auf nur einem einzigen Laufwerk speichern und dieses später dann ausfallen, so würden Sie all Ihre Backup-Daten verlieren. Aus diesem Grund sollten Sie Ihre Backup-Daten (bzw. Kopien von diesen) auf verschiedene Speichermedien verteilen, um (sinnbildlich gesprochen) nicht alles auf eine Karte zu setzen. Leider wird der TVH-Plan recht selten verwendet, weil er vielen Anwendern zu komplex und zu schwer zu verwalten ist. Gute Backup-Programme nehmen Ihnen diese komplexe Aufgabe aber vollständig ab und automatisieren sie. Ich empfehle daher die Verwendung eines Produkts, dass über diese Fähigkeit verfügt.

Backup-Software auswählen

Achten Sie bei der Auswahl Ihrer Backup-Software auf folgende wichtige Punkte:

- **Weiterreichende Wiederherstellungsfunktionen:** Es ist gut, wenn Sie Ihre Backup-Archive auch noch für mehr verwenden können, als Sie nur simpel zu speichern. Wenn Sie z. B. eine SQL-Datenbank sichern, ist es nützlich, wenn Sie auch die resultierende Backup-Datei als SQL-Datenbank einbinden können. Im Notfall können Sie sofort auf die Daten im zugreifen, ohne eine aufwendige Wiederherstellung durchführen zu müssen. Ein anderes Beispiel ist der mögliche Befall eines Systems mit einem Computer-Virus. Wenn dieser Verdacht aufkommt und Sie das Virus möglicherweise mit in einem Festplatten-Image-Backup gesichert haben, ist es hilfreich, wenn Sie das Image als virtuelles Laufwerk (in einem anderen System) mounten können. Anschließend können Sie das Virus mit einem Antiviren-Programm aus dem Image entfernen lassen – und danach das betroffene System sicher wiederherstellen.
- **Nicht erforderliche Neuinstallationen:** Anbieter von Backup-Produkten, die VMware-, Windows- oder Linux-Virtualisierungshosts nicht sichern bzw. wiederherstellen können, werden Ihnen möglicherweise sagen, dass es doch einfach sei, die entsprechenden Hypervisoren im Bedarfsfall

(bei einem Desaster) neu zu installieren. Dieser Prozess ist aber nur dann einfach, wenn Sie über alle notwendigen Programme, Fähigkeiten, Anweisungen und alle Konfigurationsparameter verfügen. Da ist es doch deutlich einfacher, wenn Sie mit einem leistungsfähigen Backup-Programm von den betreffenden virtuellen Hosts Image-Backups erstellen und im Bedarfsfall eben wiederherstellen können.

- **Hohe Kompatibilität mit unterschiedlicher Hardware:** Server waren früher ziemlich pingelig, was die Konfiguration des Betriebssystems und seine Anpassung an die Hardware anging. Es konnte sehr schnell passieren, dass ein Server bei kleinsten Hardware-Änderungen nicht mehr startete (insbesondere nach einer Wiederherstellung auf einem neuen System). Heute ist mehr Standardisierung üblich – moderen Backup-Programme und Betriebssysteme können flexibler an unterschiedliche Hardware angepasst werden.

Wenn Sie Hardware von verschiedenen Anbietern und/oder aus verschiedenen Generationen kaufen, sollten Sie darauf achten, dass Sie die von Ihnen verwendete Backup-Software auch Wiederherstellungen auf abweichender Hardware unterstützt.

- **Kompatibilität mit Virtualisierungssystemen:** Ihre Backup-Software sollte es ermöglichen, dass Image-Backups sowohl mit virtuellen wie auch physischen Systemen umgehen können und es möglich ist, die Daten bzw. gesicherten Systeme zwischen den Plattformen zu migrieren.

Verwenden Sie eine Backup-Software, die Image-Backups von Computer-Systemen auch als virtuelle Maschinen exportieren kann, die sich dann in das Verwaltungsprogramm gängiger Hypervisor einbinden lassen. Auf diese Weise können Sie bei einer notwendigen Wiederherstellung sehr schnell auf Ihre Daten bzw. das betreffende System zugreifen. Im Idealfall ist gar keine aufwendige Systemwiederherstellung notwendig, sondern sie starten das Image-Backup einfach als virtuelle Maschine (über den Hypervisor).

Backup-Medien auswählen

Bei der Auswahl der richtigen Backup-Medien müssen Sie zunächst bestimmen, wie viel Speicherplatz Sie benötigen. Die folgenden Richtlinien können Ihnen bei dieser Entscheidung helfen. Der benötigte Speicherplatz ergibt sich aus der gewünschten Anzahl an Backup-Kopien, der Aufbewahrungszeit für diese Kopien (was in manchen Branchen sogar durch entsprechende Verordnungen festgelegt ist) und daraus, wie umfangreich Ihre Daten sind und wie schnell sie verändert werden. Ein grober Richtwert für den Start ist: Der Speicherplatz für Ihre Backups sollte ungefähr 3- bis 5-mal so groß

sein wie ihr aktueller Datenbestand. Beobachten Sie den Verlauf dann über ein paar Monate und passen Sie ihn dann basierend auf dieser Erfahrung durch Hochrechnung an.

Wenn Sie es genauer ermitteln wollen, müssen Sie exemplarische Backups durchführen, um den Einfluss von Datenkomprimierung und Datendeduplizierung besser berücksichtigen zu können. Beobachten Sie über ein paar Wochen, wie viele Daten pro Tag anfallen bzw. gesichert werden müssen und wie viel Speicherplatz dabei benötigt wird. Auch hier muss natürlich noch berücksichtigt werden, wie viele Backup-Kopien Sie wie lange aufbewahren wollen (also die Aufbewahrungsrichtlinie mit eingerechnet werden).

Nach der Ermittlung des benötigten Speicherplatzes müssen Sie entscheiden, welcher Art von Backup-Medien Sie verwenden möchten. Die übliche Auswahl sind Festplatten, Bandgeräte und die Cloud. Jedes dieser Medien hat Vor- und Nachteile:

- Festplatten sind schnell, aber teuer.
- Moderne Bandgeräte sind zwar mittlerweile auch recht schnell, bei der Nachverfolgung und Verwaltung jedoch immer noch deutlich komplexer als Festplatten..

  Bandgeräte sind unter Umständen nicht so zuverlässig wie Festplatten, da die Bänder leicht beschädigt werden können. Bänder sind jedoch immer noch am günstigsten, wenn es um wirklich große Datenmengen geht (im Petabyte-Bereich).

- Die Cloud eignet sich ideal für Remote-Endpunkte und kleine Server.

  Backups sowohl lokal als auch in der Cloud zu speichern, ist eine sehr effektive und sichere Lösung. Die lokalen Backups werden für Wiederherstellungen bei kleineren Problemen verwendet – während die Sicherung in der Cloud (also einem externen Standord) gut vor einem möglichen Desaster schützt. Diese auch „Dual Protection“ genannte Zweifachsicherung (lokal und in der Cloud) entspricht der 3-2-1-Regel und ist sehr wirtschaftlich.

  Vergewissern Sie sich, dass Ihr Cloud-Anbieter auch das sogenannte „Initial Seeding“ unterstützt. Dieser Service vermeidet, dass Sie hohe Datenmengen (beispielsweise vollständige Image-Backups von Computern und Servern) über das Internet in die Cloud hochladen müssen, was je nach Bandbreite ja sehr lange dauern könnte. Stattdessen schicken Sie eine Festplatte mit dem großen Voll-Backup zum Standort des Cloud-Anbieters, der es dort für Sie auf seine Server hochlädt. Sie brauchen dann nur noch die nachfolgenden Teil-Backups (inkrementell oder differentiell) in die Cloud hochladen, was deutlich schneller geht. Für den Fall einer Wiederherstellung

sendet der Hersteller Ihnen auf Wunsch das umfangreiche Voll-Backup wieder auf Festplatte zurück.

Welche Speichermedien wählen Sie? Die Antwort lautet häufig: „Alle der oben genannten." Und richtig, alle drei Medientypen sind im Hinblick auf Kosten und Speicherplatz eine gute Wahl!

Eine bewährte Methode ist die Verwendung von zwei Medientypen, entsprechend der 3-2-1-Regel (siehe Einleitung zum Kapitel). Die Cloud wird als ein Medientyp angesehen. Sofern Sie keine sehr große Datenmengen (etwa im Petabyte-Bereich) haben oder nur über ein begrenztes Budget verfügen, stellen Festplatten und ein externer Cloud-Speicherplatz eine gute Lösung dar. Bei großen Datenmengen kann eine lokale Speicherung auf Bändern kostengünstiger sein.

In den folgenden Abschnitten erörtere ich alle drei Medientypen im Detail.

Festplatte

Festplatten haben als Backup-Geräte viele Vorteile:

- Sie sind zuverlässig.
- Als nichtflüchtige Speicher bleiben die auf ihnen gespeicherten Daten auch erhalten, wenn die Stromversorgung abgeschaltet wird.
- Sie sind schnell und bieten von allen drei Medientypen die kürzeste Wiederherstellungszeit.

Da die Kapazität von Festplatten inzwischen im Terabyte-Bereich (TB) liegt (die größten derzeit marktüblichen Festplatten zu moderaten Preisen verfügen über 6 TB (siehe Infobox „Wie viel sind 6 TB?"), kann Leistung ein Problem werden. Bei Laufwerken, die ausschließlich zur Sicherung verwendet werden, ist dies jedoch selten ein Problem, deshalb sollten Sie Laufwerke kaufen, die niedrige Kosten pro Gigabyte bieten. Oben im Abschnitt „Aufbewahrungsrichtlinie" erhalten Sie Tipps, wie Sie das richtige Speichermedium für Ihren Bedarf ermitteln.

Wenn Sie Festplatten oder Bandkassetten transportieren wollen (z. B. zu einem externen Speicherort) erstellen Sie am besten jeweils zwei Kopien. Und zwar für den Fall, dass eine Kopie beim Transport verloren gehen oder beschädigt werden sollte.

Auch SSD-Laufwerke (Solid State Drives) werden als Backup-Geräte eingesetzt, da sie schneller als Festplatten sind und langlebiger sein sollen (zumindest sind sie weniger empfindlich für mechanische Fehler). Diese Laufwerken haben jedoch Probleme bzw. ihre Besonderheiten, was häufige Schreibprozessen und Löschvorgänge angeht (Stichwort „Trim"-Funktion) –womit eine moderne

Backup-Software umgehen können sollte. Fragen Sie den Anbieter Ihrer Backup-Software, ob und wie er SSDs unterstützt. Wenn nicht, sind diese Produkte möglicherweise nicht wirklich zuverlässig.

Wie viel sind 6 TB?

Die Entwicklung der Speicherkapazitäten (und der damit verbundenen Kosten) haben im Computerbereich eine besonders hohe Dynamik. 1980 lagen die Kosten für ein einziges Gigabyte (GB) Festplattenspeicher teilweise im sechsstelligen Bereich. Heute kostet 1 GB Festplattenspeicher ca. 0,04 Euro. Sie könnten heute die gesamte während des 2. Weltkrieges genutzte Rechenleistung auf dem Soundchip einer Geburtstagskarte unterbringen. Und die gesamte für eine Apollo-Mondlandung verwendete Rechenleistung passt problemlos auf ein Smartphone. Ein Gigabyte entspricht grob ca. 100.000 E-Mails. Bei 6 TB entspricht das also rund 6.000.000.000 E-Mails.

Bandgerät

Eine gängige, regelmäßig wiederkehrende Behauptung ist, dass Bandgeräte bald keinen Absatz mehr finden. Und doch ist es den entsprechenden Anbietern bisher immer wieder gelungen, neue Bandformate mit hoher Kapazität für niedrige Kosten (pro Gigabyte) zu entwickeln. Aktuelle Bandversion wie LTO-6 (Linear Tape Open) speichert 5,6 TB pro Band. LTO-7 (16 TB) und LTO-8 (32 TB) sind in der Markteinführung. 560 Einschubfächer mit eingelegten Bändern können in einer standardmäßigen 19-Zoll-Station aufbewahrt werden. Das sind 17 PB pro Station. So hohe Kapazitäten benötigen bisher allerdings nur große Rechenzentren.

Wenn Sie Bänder extern aufbewahren, sollten Sie möglichst von jedem Band auch eine Kopie erstellen – und zwar für den Fall, dass die empfindlichen Bänder beim Transport beschädigt werden.

Cloud

Der größte Vorteil eines Cloud-Speichers ist dessen bequeme Handhabung. Sie müssen sich nicht mit dem Transport von Medien oder der Anfertigung mehrerer Kopien befassen (wie bei Festplatten oder Bändern), die beim Transport beschädigt werden könnten. Aber Cloud-Services haben auch Nachteile:

- **Sicherheit:** Informieren Sie sich, wie sicher ein von Ihnen ausgewählter Cloud-Speicher ist. Stellen Sie dem Anbieter folgende Fragen:
  - Ist die Anlage brandsicher?
  - Verfügt die Anlage über Notstromaggregate und redundante Netzwerkverbindungspunkte?
  - Wer führt Backups durch?
  - Sind die gespeicherten Daten verschlüsselt?
  - Wer hat Zugriff auf die Dateien in dem Speicherzentrum?
  - Ist die Anlage rund um die Uhr besetzt oder vollständig automatisiert?
- **Preis:** Die Preise für Cloud-Speicher können verwirrend sein. Neben Kosten für den Speicherplatz berechnen manche Anbieter auch Gebühren für die Datenübertragung.

  Cloud-Backups bedeuten nicht automatisch, dass Sie kein Personal mehr für diesen Bereich benötigen. Man sollte also nicht so leicht Personalkosten gegen die Kosten für den Cloud-Service gegenrechnen. Auch bei Cloud-Backups benötigen Sie noch Personen, die sich um die Abläufe und Ihre Systeme kümmern (Backup-Zeitpläne festlegen, Backups überwachen etc.).
- **Netzwerkbandbreite:** Sie sollten die Netzwerkbandbreite festlegen, die erforderlich ist, um die angestrebte Wiederherstellungszeit (RTO; siehe „Wiederherstellung in der Cloud“ weiter unten in dem Kapitel) zu erreichen. Ihre täglichen Backups sind kleiner als eine vollständige Wiederherstellung.

Cloud und Netzwerk haben aber auch viele Vorteile:

- Die meisten Cloud-Anbieter verfügen über eine gute Netzwerkanbindung, sodass Sie auf Ihre Daten von überall aus zugreifen können.
- Ein Netzwerk zu verwenden ist sehr praktisch.
- Sie müssen sich keine Gedanken mehr über das Speichern und Testen von Medien machen. Der Cloud-Anbieter garantiert Ihnen Zuverlässigkeit und erstellt redundante Kopien (manche Unternehmen berechnen jedoch Extragebühren für hochverfügbare Cloud-Speicher).
- Sie können bei den meisten Cloud-Unternehmen Ihren benötigten Speicherplatz flexibel und leicht anpassen.

Externe Speicherstandorte wählen

Nach dem 3-2-1-Plan (siehe Einleitung zu diesem Kapitel) sollen Sie drei Kopien Ihrer Daten aufbewahren – und zwar auf dem laufenden System, in lokalen Speicherorten und in externen Speicherorten. Sie können Festplatten und Bänder persönlich zu einem externen Speicherort transportieren (oder die Medien von einem Anbieter abholen lassen). Oder sogar eine drahtlose Übertragung der Daten vornehmen, die dann auf ein Netzwerkspeichergerät geschrieben werden. In diesem Abschnitt behandele ich ein paar dieser Optionen.

Wenn Sie einen Satz Backups auf Ihren laufenden Maschinen und einen zweiten Satz an einem externen Standort aufbewahren, müssen Sie dabei die Entfernung zwischen Ihrem Unternehmen und dem externen Standort berücksichtigen. Für die meisten Menschen sind 8 Stunden Fahrzeit/Reisezeit für solche Distanzen das Maximum und damit ein guter (maximaler) Richtwert. Wenn in Ihrem Gebiet ein hohes Risiko für Naturkatastrophen besteht (z. B. Erdbeben, Überschwemmungen, Orkane etc.) sollten Sie Ihre Daten aber noch weiter entfernt aufbewahren.

Online-Netzwerk

Wenn Sie erwägen, ein Online-Netzwerk als zweiten Standort zu verwenden, fragen Sie die Anbieter nach Datensicherheit und Netzwerkbandbreite. Berücksichtigen Sie auch, wie stark und oft sich Ihre Daten ändern. Der übliche Richtwert sind 5 % – aber Ihr Volumen kann natürlich leicht größer oder niedriger sein. Datenbanken ändern sich beispielsweise häufiger, Anwendungscode dagegen zumeist gar nicht (außer bei Updates/Upgrades).

Auch Geschwindigkeit muss berücksichtigt werden. Angenommen, Sie haben ein kleines Unternehmen mit 10 Mitarbeitern (mit je 5 GB) sowie 2 Servern (mit je 10 GB pro Tag) – das ergibt insgesamt 70 GB pro Tag sowie geschätzten 1,4 TB für das erste Backup. Weiterhin angenommen, Ihre Netzwerkgeschwindigkeit beträgt 100 Mbit/s. Dann dauern Ihre täglichen inkrementellen Backups ca. 90 Minuten zuzüglich etwaigem Netzwerkmehraufwand und Verzögerungen.

Komprimierung kann einen großen Unterschied bei der Datenspeicherung und Netzwerkübertragung machen. Wenn sich Daten auf die Hälfte ihrer Größe komprimieren lassen, lässt sich damit auch die Übertragungszeit durch das Netzwerk halbieren. Ich erörtere den Faktor „Komprimierung“ im späteren Verlauf dieses Kapitels – und zwar im Abschnitt „Aspekte der Komprimierung und Deduplizierung“.

Dark site

Zwei betriebsfähige Standorte zu haben, ist auch aus Sicherheitsaspekten eine gute Lösung. Aber viele können oder wollen sich das nicht leisten. Eine gute Alternative ist dann auch eine eine sogenannte *Dark Site*. Darunter versteht man einen externen Computerraum, der üblicherweise nicht im vollständigen Dauerbetrieb ist sowie über eine minimale Ausrüstung verfügt, insbesondere aber mit Speichergeräten bestückt ist. Alle Backups werden per Netzwerk in die Dark Site übertragen und dort gespeichert. In regelmäßigen Abständen wird die Dark Site in Betrieb genommen, um sicherzustellen, dass ein (zuvor erstellter) Disaster-Recovery-Plan funktioniert. Die gewisse räumliche Trennung der Dark Site vom eigentlichen Standort der Daten/des Unternehmens bietet zwar keine so hohe Sicherheit wie ein wirklicher zweiter, externer Standort, ist aber eine Art Zwischenlösung.

Cloud-Backup

Cloud-Backups erfreuen sich wachsender Beliebtheit bei Unternehmen, die Rechenzentren vor Ort benötigen und die Cloud für temporären Bedarf und Disaster Recovery verwenden wollen. Es wird einfach und effizient, die Cloud als zweiten Speicherort zu verwenden.

Wiederherstellung in der Cloud

Wenn Sie sich für eine Netzwerk-/Cloud-Lösung entscheiden, vergewissern Sie sich, dass Ihre Netzwerkbandbreite/Internetbandbreite ausreicht, um Ihre RTO-Ziele zu erreichen. Das erste Backup in die Cloud kann aufgrund seiner Größe länger dauern. Eine Lösung für dieses Problem ist die weiter oben schon erläuterte Option „Initial Seeding“, bei der Sie die Daten des ersten Voll-Backups per Festplatte an den Cloud-Anbieter senden (oder bei Bedarf für eine Wiederherstellung zurückgesendet bekommen).

Die „RTO“ (Recovery Time Objective) gibt an, wie lange Ihr System für eine Widerherstellung angehalten werden darf. Wenn Ihr angestrebter Wiederherstellungszeitpunkt (RPO, siehe Kapitel 2) auf vier Stunden und Ihre RTO auf zwei Stunden gesetzt sind, ist ein entsprechendes System zwei Stunden nach einem Ausfall wieder funktionstüchtig. Sie können jedoch Daten von vier Stunden verlieren, je nachdem, wie alt Ihr letzter Wiederherstellungszeitpunkt ist. Wenn Ihr System nach zwei Stunden wieder funktionstüchtig und auf dem neuesten Stand sein soll, müssen RPO und RTO gleichermaßen auf zwei Stunden gesetzt werden. RTOs können für verschiedene Subsysteme und das gesamte System unterschiedlich sein. Eine Abteilung für Auftragseingänge kann z. B. eine RTO von fünf Minuten benötigen, während die RTO für eine Lohnbuchhaltung auf zwei Tagen festgelegt wird.

Öffentliche oder private Cloud

Eine wichtige Überlegung ist, ob Sie eine öffentliche Cloud verwenden möchten. Manche Backup-Anbieter bieten Cloud-Speicher an, der speziell für die Speicherung von Backups optimiert ist. Aber auch große, öffentliche Clouds bieten größere Online-Speichermengen. Ein wichtiger Aspekt bei der Wahl des richtigen Anbieters ist auch die Frage, ob und wie leicht die Speicherkapazität flexibel angepasst werden kann.

Die Gebührenstruktur kann bei manchen Cloud-Anbietern verwirrend sein. Einige Services berechnen Ihre Gebühren pro Jahr; andere pro Monat. Manche erheben zusätzliche Gebühren für die Internetdatenübertragung oder für bestimmte Aktionen (etwa eine vollständige Datenlöschung). Vergessen Sie bei Ihrer Entscheidung für einen bestimmten Anbieter außerdem nicht die bereits diskutierten Sicherheitsaspekte.

Aspekte der Komprimierung und Deduplizierung

Komprimierung – ein Prozess zur Verkleinerung von Daten/Dateien mithilfe bestimmter Algorithmen. Üblicherweise werden dabei sich wiederholende Informationen durch Abkürzungen ersetzt. Viele Speicherspezifikationen im Computerbereich verwenden Komprimierungen. Komprimierung funktionieren allerdings nur mit „vorhersagbaren" Daten gut. Wenn der Name Ihres Unternehmens z. B. Acronis lautet und dieser Name häufig im Text vorkommt, wird dies bei der Komprimierung erkannt und eine Abkürzung für den Namen erstellt.

Viele Daten (z. B. Fotos und Videos) sind jedoch schon komprimiert und können für ein Backup nicht noch einmal effizient komprimiert werden. Und auch verschlüsselte Daten lassen sich normalerweise nicht mehr komprimieren, weil die Daten in Ihnen nicht mehr vorhersagbar sind (was ja der Sinn der Verschlüsselung ist ;-)). Wenn Sie erleben, dass verschlüsselte Daten *dennoch* komprimiert werden können, sollten Sie dem entsprechenden Verschlüsselungssystem mit großem Misstrauen begegnen.

Das Verfahren der *Deduplizierung* hat gewisse Ähnlichkeiten mit dem Prinzip der Datenkomprimierung. Wenn Sie z. B. 1.000 System-Images von Firmen-Laptops mit dem gleichen Betriebssystem sichern, werden diese zwangsläuft auch immer wieder die gleichen Betriebssystemdateien enthalten. Hier spricht man von Datenduplikaten – und ein Prozess, der es vermeidet, solche Datenduplikate mehrfach zu speichern, kann viel Speicherplatz einsparen. Bei einer solchen Deduplizierung wird nur je *eine* Kopie dieser redundanten Daten in einem speziellen „Storage" gespeichert.

In den entsprechenden, ursprünglichen Backups wird nun an der Stelle der Datenduplikate nur ein Verweis auf diese *eine* Kopie im Storage hinterlegt. Wenn die deduplizierten Daten beispielsweise Tausende von Zeichen enthalten und der Verweis auf die *eine* Kopie nur aus 20 Zeichen besteht, kann die Speicherersparnis enorm sein!

Deduplizierung funktioniert also besonders gut, wenn es eine hohe Menge an solchen mehrfachen Datensätzen gibt. Es gibt verschiedene Deduplizierungsmethoden. Ein wichtiger Unterschied ist, wo bzw. wann die Deduplizierung erfolgt. Sie kann im laufenden Betrieb (bei der Backup-Erstellung) erfolgen, sodass schon die Datenmenge reduziert wird, die in die Backup-Archive geschrieben wird. Das kann beispielsweise ein Netzwerk entlasten, weil nicht mehr so viele Daten übertragen werden müssen. Jedoch braucht der Prozess der Backup-Erstellung eine hohe Rechenleistung. Die Alternative dazu sind Verfahren, bei denen die Deduplizierung quasi als Nachbearbeitung nach der Backup-Erstellung im Storage erfolgt, der die Backup-Archive verwaltet. Beide Varianten haben unterschiedliche Ansprüche, wo genau welche Ressourcen (Rechnenleistung und Speicherplatz) benötigt werden. Wenn Sie deduplizierbare Daten haben, sollten Sie die möglichen Verfahren und ihre jeweiligen Vor-/Nachteile sorgfältig durch Tests vergleichen, um herauszufinden, wie viel Zeit, Rechen- und Speicherkapazität Sie benötigen.

Die Kosten berechnen

Es ist schwierig, die Kosten für Backup-Speicher exakt zu berechnen, aber es gibt ein paar hilfreiche Faustregeln:

- Auf Bruttospeicherebene betragen die Kosten für Festplatten ca. 0,04 Euro pro GB und für Bänder ca. 0,01 Euro pro 1 GB (was sich natürlich je nach Marktsituation schnell ändern kann)
- die meisten Cloud-Anbieter haben monatliche Gebühren, einige erheben auch Gebühren für die Datenübertragung. Zum Zeitpunkt der Erstellung dieses Buches berechnete beispielsweise Amazon ca. 0,02-0,03 Euro pro Monat für Speicherplatz und ca. 0,1 Euro pro 1 GB Netzwerkübertragung (diese Preise sind natürlich nur grobe Richtwerte und können sich marktbedingt jederzeit deutlich ändern).
- Cloud-Preise beinhalten nicht nur die Kosten für den eigentlichen Speicherplatz – sondern auch die Nebenkosten für den Betrieb (z. B. Personalkosten, Wartungskosten, Kosten für Stellplätze und natürlich den Stromverbrauch etc.). Wenn Sie diese Kosten ebenfalls zu denen für Ihren lokalen Speicher hinzufügen, können auch bei Ihnen die Gesamtkosten 5- bis 20-mal höher werden (je nach Standort und Menge des Speicherplatzes).

Über längere Zeiträume (Faustregel: ab drei Jahre) sind Bandgeräte die billigste Backup-Methode – gefolgt von Festplatten. Die Cloud erscheint vielen Anwendern zuerst einmal als teuerste Lösung – das kann jedoch eine Fehleinschätzung sein, wenn man alle Kosten und das komplette Backup-Szenario berücksichtigt. Denn Cloud-Speicher haben sehr niedrige Anschaffungskosten (eigentlich keine) und der benötigte Speicherplatz lässt sich meist flexibel anpassen. Bei klassischen Medien (Festplatte oder Band) müssen Sie bei deutlichen Kapazitätsänderungen manchmal die komplette Ausrüstung (z. B. ein NAS-System) neu kaufen. Am besten ist es, wenn Sie eine Backup-Software verwenden, die mit all diesen Speichermedien und Systemen (Festplatten, Bandgeräte, Cloud, physische, virtuelle und Cloud-basierte Systeme) umgehen kann. Dann können Sie Ihre Backup-Strategie jederzeit nach technischen oder wirtschaftlichen Gesichtspunkten anpassen.

Kapitel 4

Daten wiederherstellen

In diesem Kapitel

- Wissen, wenn Sie Daten verloren haben
- Ihren Wiederherstellungsplan zum Einsatz bringen
- Nach Einfachheit streben

Es gibt viele Gründe, warum Daten aus einem Backup wiederhergestellt werden müssen. Die häufigsten Gründe sind Anwenderfehler: versehentliche Datenlöschung, das versehentliche Überschreiben einer aktuellen Datei mit einer alten Version, verlorene Datenträger und ähnliches. Manchmal gehen Daten auch einfach deswegen verloren, weil sich niemand mehr erinnern kann, wo und unter welcher Bezeichnung eine Datei gespeichert wurde. Dann gibt es noch eine Reihe weiterer Gründe: Befall des Systems durch Viren/ Malware, Sabotage durch unzufriedene Mitarbeiter, Hardware-Probleme (z. B. defekte Festplatten), Übertragungsfehler in Netzwerken, Software-Fehler in Anwendungen und Betriebssystemen.

Unter *Datenwiederherstellung* versteht man dann den Prozess, mit dem Sie verlorene oder beschädigte Daten „zurückbekommen". Da ein Datenbestand oder ein System dabei meist aus Daten wiederhergestellt werden, die zu einem früheren Zustand als Backup gesichert wurden, spricht man auch vom „Zurücksetzen" (eines Systems oder Datenbestandes). Grundsätzlich ist es dabei egal, welcher Art die Daten sind und wie viele es sind (egal ob eine wichtige Telefonnummer oder eine ganze Server-Farm). Oder auch, durch welchen Vorfall die Daten verloren gingen (ob durch Benutzerfehler oder eine Überschwemmung des Server-Raums).

In diesem Kapitel zeige ich Ihnen, wie Sie einen sogenannten „Datenwiederherstellungsplan" Ein solcher Plan kann ihnen vor allem in Notsituationen gute Dienste leisten, wenn es zu einem echten Desaster gekommen ist und Sie unter Zeitdruck und Anspannung Ihre Daten möglichst schnell und dennoch sicher wiederherstellen müssen. Die wichtigste Voraussetzung dafür ist natürlich der Zugriff auf ein intaktes Backup.

Wenn Sie mit dem Lesen dieses Buches in diesem Kapitel begonnen haben, weil Sie gerade Ihre Daten verloren haben und kein Backup besitzen, werde ich Ihnen kaum noch helfen können. Es gibt Fälle von Datenverlusten, bei denen Ihnen aber spezielle Datenrettungsdienstleister oder Programme helfen können. Ein typischer Fallsind beschädigte Festplatten – egal ob aufgrund eines Hardware-Fehlers oder weil Sie die Festplatte vielleicht selbst versehentlich gelöscht bzw. formatiert haben. Der Erfolg solcher Anbieter bzw. Programme hängt aber immer ganz wesentlich von der Art und dem Umfang des Schadens ab. Hier kann man wenig pauschale Aussagen treffen. Daten auf Festplatten, die mit einem speziellen Programm sicher gelöscht wurden (z. B. durch gezieltes, mehrfaches Überschreiben mit Nullen und Einsen) oder die verschlüsselt wurden – und anschließend hat man das Kennwort verloren – lassen sich i. d. R. nicht wiederherstellen. In solchen Fällen kann ich Ihnen nur mein Mitgefühl aussprechen.

Datenverlust erkennen

Ein Datenverlust ist nicht immer offensichtlich. Manchmal denkt man zuerst an andere Fehler (in der Hardware oder Software) oder an mangelnde Ressourcen (z. B. zu wenig Arbeitsspeicher). Hier sind zwei Beispiele:

- **Nach einem Absturz bootet das System, aber die Anwendungen stürzen ab.** Sie können sich die Protokolle und Fehlermeldungen der Anwendungen ansehen. Außerdem haben Sie die Möglichkeit, weitere Systemüberwachungstools (z. B. des Betriebssystems) zu verwenden. Oft steht man unter Zeitdruck, weil das System zu einem bestimmten Zeitpunkt wieder lauffähig sein muss. Wenn Sie mit mehreren Anwendungen Probleme haben, kann eine vollständige Wiederherstellung lange dauern. Sie müssen also herausfinden, ob das Problem andere Ursachen hat (etwa ein installierter Sicherheitspatch oder eine Fehlfunktion in der betreffenden Anwendung) oder ob eben verwendete Daten beschädigt wurden oder sogar verloren gingen. Denn auch dies kann zu ähnlichen Symptomen führen.

Oft ist es einfacher (statt einer kompletten Wiederherstellung des Systems auf einem physischen Computer) das Backup als virtuelle Maschine (VM) zu starten (sofern vom Backup-Programm unterstützt). Wenn das nicht geht, besteht oft wenigstens die Option, das Backup als virtuelles Laufwerk zu mounten, um den Datenbestand zu untersuchen. Verlorene oder beschädigte Systemdateien lassen sich so häufig leicht(er) finden. Egal auf welche Art Sie das Problem letztendlich unter Verwendung eines Backups wiederherstellen: Sie sollten später der Ursache des Problems auf den Grund gehen, um zukünftige Wiederholungen zu vermeiden.

- **Nach einem Absturz läuft das System zwar, aber Sie erhalten Fehlermeldungen, dass Daten beschädigt wären.** In solchen Fällen ist es schwer zu entscheiden, ob hier nur ein paar bestimmte Daten verloren gingen/beschädigt wurden oder ob Sie besser direkt eine komplette Wiederherstellung vornehmen sollten. Oft ist es einfacher (sofern man ein aktuelles, vollständiges Backup hat), das betreffende System komplett wiederherzustellen, statt sich zu lange mit der Fehlersuche aufzuhalten.

Es ist ein gängiger Fehler, sich zu lange mit einer Fehlersuche aufzuhalten. Sie können meist viel Zeit sparen, wenn Sie ein oder mehrere vollständige Backups des Systems haben – und das System so im Bedarfsfall jederzeit schnell und einfach auf einen Zustand zurücksetzen können, in dem der Fehler noch nicht auftrat.

So oder so gibt es quasi ein klares Computergesetz: Früher oder später trifft es jeden! Sie (wie alle anderen auch) werden früher oder später ebenfalls Daten verlieren – es ist nur eine Frage der Zeit! Datenverlust tritt oft in einem geringfügigen und überschaubaren Maß auf, jedoch häufiger als den meisten bewusst ist. Viele Kleinunternehmen geben an, ein- oder zweimal pro Woche Daten wiederherstellen zu müssen. Ein Benutzer hat vielleicht eine wichtige E-Mail gelöscht, ein anderer vermisst eine vor Monaten erstellte Präsentation. Gehen wichtige Daten verloren, die nicht wiederhergestellt werden können, so müssen sie erneut erstellt werden. Was oft schwer, zeitaufwendig und manchmal sogar unmöglich ist.

Schwieriger als die Wiederherstellung einzelner Dateien kann die Wiederherstellung eines kompleten Systems sein, das beispielsweise aufgrund eines fehlerhaften Updates beschädigt wurde. Ein guter Wiederherstellungsplan kann die Komplexität dieser Aufgabe aber deutlich reduzieren bzw. handhabbarer machen.

Auch wenn die meisten Wiederherstellungsaktionen aufgrund von Benutzerfehlern erfolgen und oft nur wenige Dateien betreffen, sollten Sie darauf vorbereitet sind, auch eine komplette Systemwiederherstellung durchführen zu müssen. Für solche Fällen sollten Sie mit einer guten Backup-Prozedur und einem Wiederherstellungsplan gewappnet sein. Denken Sie an die im letzten Abschnitt erwähnte Empfehlung: es ist meistens effektiver (weil zeit- und nervenschonend), ein komplettes System wiederherzustellen, statt sich zu lange mit einer detaillierten Fehlersuche aufzuhalten, die nur zu häufig erfolglos ist. Nach Albert Einstein ist die Definition von Wahnsinn, „immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten“. Die meisten Anwender waren schon mal an dem Punkt, dass sie es einfach nicht wahrhaben wollten, ein System aufgrund verlorener Daten beschädigt zu haben – und stattdessen immer wieder versucht haben, das System neu zu starten. Machen Sie sich

in so einem Fal nicht auch „wahnsinnig“, stellen Sie Ihr System lieber direkt aus einem entsprechenden Backup wieder her!

Ein guter Rat in diesem Zusammenhang ist es, Wiederherstellungsprozeduren zu üben. Durch so einer Übung können Sie ermitteln, ob Sie über alle benötigten Daten, Programme und Anweisungen verfügen. Außerdem erhalten Sie die notwendige Sicherheit, um im Bedarfsfall eine Wiederherstellung schnell und ohne allzuviel nervliche Anspannung durchführen zu können.

Achten Sie darauf, dass Ihre Backups und Backup-Medien intakt sind und bleiben. Denn auch die Backup-Archive selbst sowie die für sie verwendeten Speichermedien können beschädigt werden. Fehler auf Speichermedien können sich außerdem auf Backup-Archive übertragen. Ein typisches Beispiel sind Dateisystemfehler auf einer Festplatte, von der dann ein Image-Backup erstellt wird. Wenn das Laufwerk aufgrund eines weiteren Fehlers komplett ausfällt, greift man auf das erstellte Image-Backup zurück – und muss leider feststellen, dass auch dieses beschädigt ist, weil sich der Fehler übertragen hat. Es empfiehlt sich daher, Backup-Archive nach der Erstellung und auch regelmäßig während ihrer Speicherung zu validieren – gute Backup-Programme verfügen über solche Validierungsfunktionen. Um ganz auf Nummer sicher zu gehen, sollten Sie auch die verwendeten Speichermedien regelmäßig prüfen und/oder zusätzliche Kopien auf anderen Medien erstellen (siehe die in diesem Buch schon öfter erwähnte 3-2-1-Regel).

Ihren Wiederherstellungsplan in Gang setzen

Ich hoffe, dass Sie über schriftliche Wiederherstellungsprozeduren verfügen, die Sie regelmäßig üben. Mit so einem Plan können Sie im Falle eines Datenverlusts Daten schnell und einfach wiederherstellen.

Einige Backup-Programme ermöglichen es, die Wiederherstellungsprozedur auszudrucken. Dies ist durchaus ratsam, denn so ein Ausdruck ist oft schneller zur Hand und übersichtlicher als eine gespeicherte Version, die auf irgendeinem Datenträger „herumfliegt“. Gerade unter Eile und Druck ist ein solcher Plan auf Papier etwas, was die Nerven beruhigt.

Mit einem guten Wiederherstellungsplan ist auch die Wiederherstellung in einem komplexen Umfeld (z. B. von virtuellen Systemen im Unternehmensumfeld) in der Regel ein einfacher Prozess. Eine solche Prozedur, die man mit einem Wiederherstellungsplan verfolgt, kann beispielsweise so aussehen:

1. **Starten Sie das Hostsystem, das Sie mit dem Backup-Programm verwenden wollen.**
2. **Stellen Sie den Hypervisor und wenn möglich die VMs auf der Festplatte des Hosts wieder her.**
3. **Starten Sie den Host.**
4. **Starten Sie die VMs oder stellen Sie diese aus einem anderen Backup-Satz wieder her und starten Sie sie dann.**

Insbesondere wenn Sie die Schritte vorher geübt haben, sollte der Ablauf nicht lange dauern und erfolgreich verlaufen!

Sie sollten eine Person bestimmen, die speziell für Wiederherstellungen verantwortlich ist und sich um alle notwendigen Aktionen kümmert. Wenn zu viele Personen involviert sind und widersprüchliche Schritte vorgenommen werden, kann der Prozess leicht fehlschlagen („viele Köche ...“ usw). Im Unternehmensumfeld und für komplexe Systeme gibt es natürlich auch spezielle Anbieter, die diese Aufgabe für Sie als Dienstleistung übernehmen können. Ideal ist es, wenn die Wiederherstellungsprozedur außerdem eine Funktion beinhaltet, mit der man das System bereits nutzen kann, während die Aktion noch läuft. Eine typische Bezeichnung für eine solche Funktion ist „Active Restore“. Insbesondere bei Systemen, die sich im Dauerbetrieb befinden sollen (z. B. Server) ist eine solche Option sehr nützlich.

Halten Sie die Dinge einfach

Ich möchte Sie noch einmal auf das Problem einer zu hohen Komplexität hinweisen. Backup- und Wiederherstellungslösungen sollten möglichst einfach und übersichtlich sein, um Anwendungsfehler sowie Inkompatibilitäten zu vermeiden. Am besten ist es, wenn alle Funktionen aus einer Hand bzw. unter einer Oberfläche gebündelt sind. Eine gute Lösung (vor allem im Unternehmensumfeld) sollte Backup und Wiederherstellung für physische, virtuelle und Cloud-Umgebungen sowie für Windows, Linux und granuläre Anwendungen bereitstellen kann. Und natürlich auf allen relevanten Ebenen Image-Backups unterstützen. Eine solche integrierte Lösung ist weit sinnvoller, als diverse Einzellösungen einzusetzen, bei denen sich beispielsweise ein Produkt um die Wiederherstellung von Microsoft Exchange kümmert und ein anderes um SQL-Datenbanken. Die Verwendung mehrerer Anbieter und Systeme kann verwirrend sein und bietet weniger Interoperabilität. Sie müssen Prozeduren häufiger aktualisieren und ändern.

Kapitel 5

Backup-Verwaltung

In diesem Kapitel

- Im Hinblick auf Technologie auf dem neuesten Stand bleiben
- Wissen, was gesichert werden muss – und wann
- Ihre Arbeit planen und Ihren Plan zum Einsatz bringen

Das Geheimnis erfolgreicher Backups und Wiederherstellungen liegt darin, die richtigen Prozeduren zu entwickeln und Vorgänge bzw. Abläufe sorgfältig zu planen. Denken Sie daran, dass Sie selbst bei einem Datendesaster (z. B. einem Systemausfall) quasi die letzte Rettung sind. Es liegt oft am Anwender selbst, wie gut und schnell eine Wiederherstellung funktioniert. Sie sollten sich also auf den Tag vorbereiten, an dem alles schief geht. Und nach Murphy's Law geht dann bekanntlich wirklich *alles* schief ;-).

Ihre Aufgaben sind an sich einfach und bestehen im Wesentlichen aus zwei Dingen:

- Stellen Sie sicher, dass ein guter Backup-Plan verfügbar ist – und sorgen Sie dafür, dass er auch wirklich ausgeführt wird.
- Stellen Sie sicher, dass ein guter Wiederherstellungsplan vorhanden ist – und überprüfen Sie dessen Wirksamkeit.

In diesem Kapitel zeige ich Ihnen, wie Sie dabei vorgehen sollten.

Im Hinblick auf Backup-Produkte auf dem Laufenden bleiben

Mit Informationen fängt alles an: Versuchen Sie, bei allen relevanten Aspekten stehts auf dem neuesten Stand zu bleiben. Dies betrifft insbesondere die verwendeten Backup-Produkte, die eingesetzte Hardware und weitere, dabei benötigte Software. Insbesondere die verwendete Software sollte immer auf dem neuesten Stand sein (mit allen Updates und Upgrades). Ja, dieser Anspruch kann schon viel

Arbeit bedeuten – nicht nur, weil den Produkten mit neuen Versionen auch meist neue Funktionen hinzugefügt werden, sondern auch, weil sich die Art und Weise ändert, in der Informationstechnologie verwendet wird. Daher werden im Unternehmensumfeld auch spezielle Administratoren mit dieser Aufgabe betreut. Privatanwender und Freiberufler müssen meist „ihr eigener Admin" sein. Umso wichtiger ist es aber gerade auch hier, sich durch aktuelle Produkte vor Ärger zu schützen.

Allein der Bereich „Virtualisierung" ist so stark gewachsen in den letzten Jahren, sodass entsprechende Backup-Produkte über viele neue Funktionen und Möglichkeiten verfügen. Was Sie außerdem vor allem im Unternehmensbereich im Blick halten sollten, sind folgende Bereiche: softwaredefinierte Speichersysteme, das „Internet der Dinge" und die zunehmende Verschmelzung von Entwicklung und Betrieb. All diese neuen Technologien werden großen Einfluss auf die Funktionen von professionellen Backup-Programmen haben.

Sie sollten Ihre Backup-Planung langfristig ausrichten und mit der allgemeinen IT-Planung Ihres Unternehmens abstimmen. Die zunehmende Nutzung von „Software as a Service" (SaaS), von Virtualisierung und verteilten, dezentralen Speicherorten haben sowohl Einfluss auf die allgemeine IT-Planung wie auch auf die Backup-Prozeduren.

Das Backup-Fenster festlegen

Die nächste Aufgabe ist vielleicht die schwierigste. Sie besteht darin, den angestrebten Wiederherstellungszeitpunkt (RPO) festzulegen, diesen in das Backup-Fenster einzupassen und die angestrebte Wiederherstellungszeit (RTO) einzuhalten. (RPO wurde in Kapitel 2 behandelt, RTO in Kapitel 3.) Um dies zu tun, müssen Sie Folgendes festlegen:

- Die wichtigsten Anwendungen, die Sie sichern möchten
- Die mit diesen Anwendungen verbundenen (aktuellen und voraussichtlichen) Datenmengen
- RPO und RTO der Anwendungen

Anhand dieser Informationen können Sie ermitteln, wie viel Zeit Sie den jeweiligen Backups einräumen müssen. Leider kann es vorkommen, dass Backups die Ressourcen belasten, Anwendungen daher langsamer ausgeführt werden oder sogar Arbeitspausen notwendig sind. Eine gängige (jedoch nicht so empfehlenswerte) Vermeidungsstrategie besteht darin, die Backups außerhalb der üblichen Stoßzeiten auszuführen. Dummerweise erfolgen die meisten Datenänderungen aber genau innerhalb dieser Stoßzeiten – und sind Backups also genau hier am wichtigsten!

Es gibt keine allgemeingültige Antwort auf die Frage, wie viel Zeit ein Backup in Anspruch nehmen sollte. Vergewissern Sie sich, dass Sie über ausreichend Ressourcen verfügen, um im normalen Betrieb auch ein Backup ausführen zu können.

Einen Backup-Plan erstellen und überprüfen

Kurze Wiederherstellungszeiten, häufige Wiederherstellungspunkte und eine langfristige Aufbewahrung erfordern ein kluges Vorgehen. Hier ein paar Ideen, die nützlich sein können:

- Hybride lokale Speicher sowie Cloud-Speicher (siehe Kapitel 3) können helfen, die Daten zu reduzieren, die zu einem zweiten Speicherort verschoben werden müssen.
- Der Aufbewahrungsplan „Türme von Hanoi“ (TVH, siehe Kapitel 3) kann sicherstellen, dass Sie sowohl über häufige, aktuelle Wiederherstellungspunkte verfügen – wie auch über ältere. Dadurch sind Sie auch vor schleichenden Datenbeschädigungen geschützt, die sich möglicherweise schon länger in Ihrem System befinden, aber erst nach längerer Zeit bemerkt werden. Und so etwas kommt häufiger vor, als die meisten denken.
- Nutzen Sie Deduplizierung und Komprimierung, um die Speicheranforderungen zu reduzieren (siehe Kapitel 3).
- Nutzen Sie Image-Backups in Kombination mit inkrementellen Backups und einer Konsolidierungsprozedur, um die Speicheranforderungen zu reduzieren. Insbesondere, weil diese Maßnahmen wirken, ohne die RTO (siehe Kapitel 2) zu beeinträchtigen.

Erstellen und nutzen Sie einen gut durchdachten Backup-Plan! Ihre Backup-Lösung sollte möglichst über eine zentrale Verwaltungskonsole verfügen, die einen Haupt-Backup-Plan für jedes System anpassen und auf dem System installieren sowie seinen Fortschritt überwachen und ihn auf Fehler untersuchen kann.

Die Dinge einfach halten (oder nicht)

Ein Backup-Plan kann ganz einfach sein und folgendermaßen lauten: Täglich um Mitternacht ein vollständiges Backup von allen Daten durchführen. Ein Plan kann aber auch sehr komplex sein und dann folgendermaßen lauten:

> Für Auftragseingänge wöchentlich ein vollständiges Backup und stündlich ein inkrementelles Backup durchführen. Für Bestandskontrollen alle 15 Minuten ein Backup nur von der

Datenbank durchführen. Für die Fertigungssteuerungen alle vier Stunden ein vollständiges Image-Backup durchführen. Für alle Benutzerendpunkte monatlich ein vollständiges Backup durchführen, an der Quelle eine Deduplizierung vornehmen, alle 12 Stunden ein inkrementelles Backup mit Verschlüsselung und Komprimierung jedes Benutzerverzeichnisses durchführen, aber die Zeiten zufällig festlegen, damit nicht alle gleichzeitig erfolgen.

Je komplexer die RPOs und RTOs eines Unternehmens sind, desto komplizierter wird ein dazugehöriger Backup-Plan. Um diese Komplexität so gering wie möglich zu halten, empfiehlt es sich, möglichst nur ein integriertes Backup-Programm zu haben (statt vieler verschiedener, von unterschiedlichen Anwendern), das alle notwendigen Aufgaben in einen zentralen Backup-Plan vereinen kann.

Backup-Fenster festlegen

Ein Backup-Fenster ist diejenige Zeitspanne, in der ein System angehalten oder verlangsamt wird, um ein Backup durchführen zu können. Wenn Ihr Produktionsunternehmen beispielsweise in zwei Schichten arbeitet, könnte ein typisches Backup-Fenster acht Stunden betragen (in der Pause zwischen zwei Schichten zu je 8 Stunden). Wenn ein Unternehmen jedoch rund um die Uhr arbeitet, müssen auch alle Backups während der Betriebszeiten ausgeführt werden – und beeinflussen unter Umständen die Ressourcen der Systeme.

Backup-Technologien werden zwar laufend verbessert, aber eine perfekte Lösung für Backups ohne Backup-Fenster gibt es bisher nicht (und das wird wohl vorerst auch so bleiben). Eine häufige Lösung ist die Verwendung mehrerer, kurzer Backup-Fenster, die man an unterschiedliche Arbeitslasten anpasst. Leistungsfähige Backup-Produkte helfen bei dieser Aufgabe, indem eine zentrale Verwaltungskonsole hilft, die benötigten Backup-Fenster zu optimieren und zu automatisieren.

Die Anbieter hochwertiger Backup-Produkte stellen eine zentrale Verwaltungskonsole bereit, mit der Sie einen Backup-Plan erstellen und für dessen Ausführung bestimmte Zeiten festlegen können. Auf diese Weise können sie leichter gewährleisten, dass nicht alle Backups gleichzeitig ausgeführt werden und somit die Ressourcenbelastung möglichst gering ist. Ein Backup-Plan sollte es auch ermöglichen, dass neu hinzugekommene Maschinen, Server oder höhere Arbeitslasten leicht in einen bereits vorhandenen Backup-Plan (durch eine entsprechende Anpassung) übernommen werden können. Ebenfalls wichtig ist die Berücksichtigung einer Deduplizierungsfunktion, um Speicherplatz zu sparen. Dazu müssen

Sie die Zahl und Speicherorte der Archive und dazugehörigen Storage-Depots („Vaults“) nutzen und anpassen können. Stellen Sie außerdem sicher, dass die Backup-Schreibvorgänge auf genügend Ressourcen verteilt werden, um die Belastung für das Netzwerk und die einzelnen Systeme so gering wie möglich zu halten.

Die Ausführung überprüfen

Die Ausführung eines Backup-Plans sollte überwacht und überprüft werden, um sicherzustellen, dass keine Backups fehlschlagen oder um die Ursache möglicher Fehler ermitteln zu können. Typische Fehlerursachen sind unzureichender Speicherplatz im Storage, der als Ziel verwendet wird und Netzwerkprobleme. Ein Backup-Plan sollte auf solche Probleme vorbereitet sein, sie erkennen und entsprechende Fehlermeldungen ausgeben können oder sogar Gegenmaßnahmen einleiten können (z. B. ein alternatives Notfall-Backup oder das Senden einer Benachrichtigung an einen Administrator mit der Aufforderung zum Eingreifen).

Den Plan überwachen

Auch wenn ein Backup-Plan perfekt erstellt wurde, die entsprechenden Backups automatisch ausgeführt werden, eine Kapazitätenverwaltung vorhanden ist und die Netzwerkleistung zuverlässig ist, verbleiben noch wichtige Aufgaben:

- **Auf Änderungen achten.** Moderne, Cloud-basierte und mit Virtualisierung arbeitende Rechenzentren können Benutzern helfen, Arbeitslasten leichter aufzuteilen. Dabei ist es immer möglich, dass in der virtuellen Umgebung auch neue virtuelle Maschinen (VMs) auftauchen. Die Backup-Verwaltung des entsprechenden Produkts sollte in der Lage sein, solche neuen VMs zu erkennen und zu sichern.
- **Den Bestand erfassen.** Erfassen Sie Systeme, Festplatten und Archive, um sicherzustellen, dass alles, was gesichert werden muss, auch gesichert ist.

Kapitel 6

Zehn Dinge, die Sie über Backups wissen sollten

In diesem Kapitel

- Kosten verstehen
- Prioritäten festlegen
- Wissen, was wann zu tun ist

Wenn Ihre Backups konsistent sind, alle wichtigen Parameter regelmäßig überprüft werden und Sie Ihre Wiederherstellungsprozeduren geübt haben, sollte Sie auch ein Notfallanruf um 02:00 Uhr in der Nacht nicht mehr aus der Ruhe bringen können. Wenn Sie auf eine solche Situation vorbereitet sind, können Sie auch sicher mit dem Problem umgehen. In diesem Kapitel fasse ich noch einmal die zehn wichtigsten Aspekte zusammen, die Sie wissen sollten, um Backups und Wiederherstellungen so einfach und effizient wie möglich zu gestalten.

Der Wert Ihrer Daten

Egal ob Unternehmen oder Privatanwender: zumeist liegen viele Arten von Daten vor. Einige Daten ändern sich langsam, andere schnell. Einige Daten stehen beispielsweise im Zusammenhang mit einem Verkauf, andere mit einem Produkt oder einer Dienstleistung, wieder andere mit Finanzberichterstattungen, Marketing oder Personalwesen. Zu wissen, wie wichtig jeder Datentyp ist und wie häufig sich die betreffenden Daten ändern, hilft Ihnen, einen passenden Wiederherstellungszeitpunkt (RPO) für diese Daten zu ermitteln.

In der Regel passen Unternehmen den RPO an unterschiedliche Arbeitslasten und Anwendungen an. Weitere Informationen zum RPO können Sie dem Kapitel 2 entnehmen.

Die Kosten von Ausfallzeiten

Eine entsprechende Berechnung ist häufig einfach – jedoch nicht immer. Wenn beispielsweise ein Fertigungssystem ausfällt, lassen sich die Kosten für untätige Mitarbeiter und nicht mehr hergestellte Produkte leicht summieren. Wenn dagegen das Reservierungssystem einer Fluggesellschaft ausfällt, ist die Ermittlung der Ausfallskosten nicht mehr so einfach. Neben verlorenen Einnahmen, weil keine Flugplätze mehr reserviert werden können, kann der Vorfall auch Kunden verärgern und den guten Ruf des Unternehmens schädigen. Im schlimmsten Fall drohen sogar Regresszahlungen. Die Kosten für Ausfallszeiten hängen also vom jeweiligen Geschäftsbereich ab. Unabhängig davon sind Daten (bzw. ihre Verfügbarkeit) aber zumeist generell wertvoll, auch wenn dieser Wert sich nicht immer genau in Euro und Cent ausdrücken lässt. Backup-Prozesse sind unerlässlich, um Daten und ihre Verfügbarkeit zu gewährleisten.

Nach einer von der IDC in den USA durchgeführten und von Acronis unterstützten *Studie zum Thema Disaster Recovery* (von Mai 2014) gaben mehr als 90 % aller Unternehmen die Kosten von Ausfallzeiten mit mehr als 20.000 USD pro Stunde an. Fast die Hälfte aller amerikanischen Unternehmen meldete Kosten in Höhe von mehr als 60.000 USD pro Stunde.

Arbeitslast-Prioritäten

Bei einem Totalverlust Ihres Systems bzw. Ihrer Daten kann der Wiederherstellungsaufwand stark ansteigen. In solchen Fällen empfiehlt es sich, die Wiederherstellungsprozesse aufzuteilen und je nach Wichtigkeit zu priorisieren. Folgendes muss dabei in Betracht gezogen werden:

- Die Reihenfolge, in der die jeweiligen Arbeitslasten auftreten und wie diese zu gewichten sind
- Welche Arbeitslasten haben eine hohe Priorität und sollten daher über Redundanz und Failover verfügen
- Welche Arbeitslasten haben eine niedrige Priorität und können daher beispielsweise auch ein paar Tage warten
- Welche Arbeitslasten können angehalten werden, um deren Kapazität für andere (wichtigere oder ausgefallene) Arbeitslasten bereitzustellen

So speichern Sie Ihre Backups

Eine bewährte Richtlinie für die Wahl der richtigen Speicherorte und Speichermedien ist die 3-2-1-Regel: also drei Kopien, zwei Medientypen und eine extern gespeicherte Kopie (siehe Kapitel 3). Im Idealfall verfügen Sie neben Ihrem aktuell laufenden System noch über eine weitere Kopie, die offline (aber lokal) vorhanden ist – sowie über eine weitere Kopie, die sich an einem externen Standort befindet. In jedem Fall sollten Sie darauf achten, dass alle Backup-Archive und Speichermedien sicher und gut geschützt gelagert werden.

Die Aufbewahrungszeit von Backups

Speicherplatz ist immer eine begrenzte Ressource. Auch Backups müssen daher früher oder später gelöscht werden. Diese Löschvorgänge sollte nach einer festgelegten Aufbewahrungsrichtlinie erfolgen und möglichst automatisiert werden (siehe Kapitel 3). Drei Dinge sind dabei zu berücksichtigen:

- **Rechtliche Anforderungen:** Einige Unternehmen müssen ihre Datensätze für bestimmte Zeiträume aufbewahren. Diese Anforderungen können auf Rechtsvorschriften (in regulierten Branchen) oder auf Verträgen (zwischen dem Unternehmen und seinen Kunden) basieren.
- **Wie lange werden Dateien aus funktionellen Gründen gebraucht:** Im Durchschnitt kommunizieren Unternehmen mit Kunden (per E-Mail und Dateien) über einen Zeitraum von drei Monaten. Die meisten Aufträge sind also in diesem Zeitrahmen beendet. Unter diesem rein funktionellen Aspekt reicht es in der Regel aus, die Backups dieser Daten nur vier bis sechs Monate aufzubewahren. Rechtliche Aspekte (z. B. steuerliche Gründe) können hier natürlich längere Aufbewahrungszeiten erfordern.
- Versionsverwaltung: Viele Dateien werden häufig überarbeitet. Je nach Wichtigkeit ist eine Versionsverwaltung („Versionierung“) notwendig, um die verschiedenen Stadien der Bearbeitung festzuhalten. Es ist aber nicht immer notwendig (v. a. über eine längere Zeit), auch wirklich alle Versionen aufzubewahren. Oft reicht es nach Abschluss eines Projektes, dass nur die finale Version eines Dokumentes aufbewahrt wird – alle Zwischenversionen können daher gelöscht werden. Auch dies wird am besten über eine Aufbewahrungsrichtlinie automatisiert (sofern entsprechende Parameter verfügbar sind)..

Wissen, welche Wiederherstellungs-Tools wann zu verwenden sind

Um eine System neu aufzsetzen, benötigen Sie viele Komponenten: Hardware, Backups, Installationsmedien von Betriebssystem und Anwendungen, Updates und Patches für Betriebssystem und Anwendungen – und nicht zuletzt die von Ihnen und den Anwendungen benötigten Daten. Mit Datei-Backups allein lässt sich so eine Systemeinrichtung/Systemwiederherstellung nicht sinnvoll durchführen. Wesentlich besser geeignet sind vollständige Image-Backups, denn diese enthalten alle wichtigen Daten und Metadaten.

Die Einzelheiten Ihres Backup-Plans

Aus vielen Gründen sind gut dokumentierte Wiederherstellungsprozeduren ratsam. Hier einige Szenarien, aus denen das offensichtlich wird:

- Wenn ein Geschäftsführer mitten in der Nacht versehentlich eine Datei löscht, muss er wissen, wen er anrufen soll.
- Die Person, die der Geschäftsführer anruft, muss wissen, wie die Datei wiederherzustellen ist.
- Bei einem umfangreicheren Problem muss das technische Personal wissen, wo sich das Backup befindet, welche Server wiederhergestellt werden müssen und auf welche Art.

Wenn ausgeschlossene Daten zum Problem werden

Ein häufiges Problem ist Folgendes: weil der Speicherplatz eng wird, schließen Firmen-Administratoren aus den regelmäßig erstellten Backups bestimmte Dateien aus, von denen sie annehmen, dass sie nicht benötigt werden oder nicht so wichtig sind. Bei dieser Entscheidung kommt es aber oft zu Fehlern – und im Fall einer wichtigen Wiederherstellung erweist sich dann, dass genau diese ausgeschlossenen Daten doch wichtig waren. Dann ist es aber natürlich zu spät.

Tatsächlich gibt es natürlich Daten, die üblichwerweise ohne Probleme von Backups ausgeschlossen werden können (z. B. die Auslagerungsdatei des Betriebssystems). Wenn man aber sehr viele Dateien z. B. von einem System-Backup ausschließt, kann es sein, dass man leicht einen Fehler macht und am Ende ein wiederhergestelltes System nicht läuft. In der Regel sollte man daher gut

abwägen, ob man für die Einsparung einiger Euro für zusätzlichen Speicherplatz ein solches Risiko eingehen möchte. Es empfiehlt sich meistens eher nicht, mit umfangreichen Ausschlusslisten zu arbeiten. Stattdessen sollte man eher in die Aufrüstung des Speicherplatzes investieren.

So (und in diesem Umfang) testen Sie Backups

Es empfiehlt sich, die Wiederherstellbarkeit von Backups durch entsprechende, möglichst automatisierte Testroutinen zu überprüfen. In vielen Unternehmen gibt es bereits ähnliche Testroutinen, um die Leistung bestimmter Systeme zu überprüfen. Auf ähnliche Weise sollten auch solche Wiederherstellbarkeitstests für Backups etabliert werden. Ungenutzte Server oder freie Kapazitäten in einer virtuellen Umgebung bieten sich an, um diese Testszenarien zu automatisieren. In diesen Tests sollte geklärt werden, ob sich vorhandene Backups wiederherstellen lassen, ob gespeicherte Backups intakt sind, ob die zur Speicherung verwendeten Medien intakt sind (insbesondere Festplatten können leicht überprüft werden) und ob nach einer Wiederherstellung die Dateigrößen mit den gespeicherten Kopien identisch sind.

So formulieren Sie Fragen zum Backup

Bei der Etablierung von Backup-Routinen tauchen natürlich immer wieder eine Menge Fragen auf. Beispielsweise, welche Medien man am besten verwendet oder welcher Aufbewahrungsplan sinnvoll ist. Um diese Fragen möglichst gut zu beantworten, gibt es eine Faustregel: betrachten Sie die Fragestellung nicht aus der Perspektive des Backups, sondern möglichst immer aus der Perspektive einer möglichen Wiederherstellung. Wie ist das gemeint? Nehmen wir zwei Beispiele:

- Statt zu fragen, mit welchen Speichermedium man ein Backup am besten erstellt, sollten Sie sich fragen, welches Medium sich am besten für eine später erforderliche Wiederherstellung am besten eignet
- Statt zu fragen, welche Aufbewahrungsregel die Backup-Erstellung erleichtert, sollten Sie sich fragen, welche Aufbewahrungsregel Ihnen beispielsweise auch die Wiederherstellung alter Datenbestände sicher ermöglicht. Eine solche Aufbewahrungregel wäre beispielsweise das GVS-Szenario, das in Kapitel 3 behandelt wurde.

Es nützt wenig, Backups zu optimieren, wenn dies zu Problemen bei der Wiederherstellung führt. Betrachten Sie Fragen rund um die richtige Backup-Erstellung möglichst immer aus der Perspektive einer möglichst optimalen Wiederherstellung.

Über Acronis

Acronis setzt Standards für Data Protection der Neuen Generation. Mit seinen Lösungen für Backup, Disaster Recovery und sicheren Zugriff basierend auf der AnyData Engine und dem Vorsprung durch seine Imaging-Technologie bietet Acronis einfaches, umfassendes und sicheres Backup für Dateien, Applikationen und Betriebssystem in beliebiger Umgebung, - virtuell, physisch, Cloud oder mobil.

Acronis wurde 2002 gegründet und schützt Daten von über 5 Millionen Nutzern und 300.000 Unternehmen in über 130 Ländern. Acronis-Produkte beinhalten mehr als 100 Patente und wurden u.a. zum besten Produkt des Jahres gewählt von Network Computing, TechTarget und IT Professional. Die Produkte decken eine große Bandbreite von Funktionen ab, wie z.B. Migration, Klonen und Replizierung.

Weitere Informationen finden Sie unter **www.acronis.de**. Folgen Sie Acronis auf Twitter: **http://twitter.com/acronis_de**.

Verlieren Sie nie wieder eine Datei!

Die Art, wie Sie Ihre Daten am besten sichern sollten, hat sich mit der Zeit verändert. Heutzutage werden Daten werden auf physischen Servern, Desktop-PCs, Notebooks, virtuellen Maschinen und in der Cloud gespeichert. Mit dem Erscheinen neuer Technologien mussten sich auch die Techniken ändern, um Informationen zu sichern und bei Datenverlust wiederherstellen zu können.

- ***Modernes Backup und Recovery* — lernen Sie Data Protection der Neuen Generation kennen**
- ***Einen Backup-Plan erstellen* —wichtige Aspekte und Herangehensweise**
- ***Virtuell, physisch und Cloud* — sichern Sie eine beliebige Umgebung**
- ***Flexible Wiederherstellungsoptionen* — Dateien, Applikationen und vollständige Systeme**

Sie erfahren:

- **Ein Einstieg in das Thema „Data Protection“**
- **Wie Sie Daten für ein Backup richtig erfassen**
- **Wie Sie Ihr Backup sicher speichern**
- **Vielfältige Wiederherstellungsmöglichkeiten**

Joel Berman arbeitet seit über 40 Jahren in der IT. Er hat für einige der weltweit größten Finanzinstitute und Telekommunikationsfirmen gearbeitet, und in diesen Unternehmen für Zuverlässigkeit und Integrität der Informationstechnologie gesorgt.

WILEY

ISBN 978-1-119-10179-6