# Backup / Recovery / Disaster Recovery

Leitfaden

www.bitkom.org

bitkom

## Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

## Ansprechpartner:

Christian Herzog | Bereichsleiter Technische Regulierung und IT-Infrastruktur
T +49 030 27576-270 | c.herzog@bitkom.org

## Verantwortliches Bitkom-Gremium

AK Server, Storage, Networks

## Autoren

Dieser Leitfaden wurde ab Herbst 2014 bis Jahresanfang 2016 inhaltlich von einem speziell für dieses Fachthema gebildeten Expertenkreis verschiedener Bitkom-Mitgliedsfirmen erarbeitet.

Zum Gelingen haben viele beigetragen. Besonderer Dank gilt den folgenden (alphabetisch genannten) Autoren für Ihre inhaltliche Expertise:

- Andre Gaschler, IBM
- Attila Mester, Oracle
- Claus Wiefel, Dell Software
- Dieter Unterseher, NetApp
- Norbert Postler, Fujitsu
- Stefan Bösner, Dell Software
- Stefan Ehmann, HDS
- Thomas Ruppel, Veritas

Die rechtlichen Grundlagen (Anlage) wurden erarbeitet durch:

- Heiko Gossen, Geschäftsführender Gesellschafter, migosens GmbH
- Dr. Hartmut Hässig, Datenschutzbeauftragter, EMC Deutschland GmbH
- Rudi Kramer, Rechtsanwalt, DATEV eG
- Gesa Diekmann, Leiterin Wissenschaftlicher Dienst Bitkom e.V.

# Inhaltsverzeichnis

# 1 Einleitung

# 1 Einleitung

## Präambel: Ziel dieses Leitfadens

In der heutigen Zeit speichern und nutzen Unternehmen mehr Daten als je zuvor und die Datenmengen wachsen exponentiell. Die zunehmende Abhängigkeit der Unternehmen von ihren Daten und IT-Prozessen, erfordert immer mehr Daten für längere Zeiträume aufzubewahren. Der gleichzeitige Wettbewerbsdruck steigt und erfordert von den Unternehmen effizientere Methoden einzuführen, um ihre Daten wirtschaftlich zu verwalten und vor Verlusten und Nichtverfügbarkeit zu schützen. Dies erfordert von den zuständigen IT Abteilungen oder Dienstleistern auch bei dem Thema Datensicherung (Backup) und Wiederherstellung (Restore) leistungsfähigere und flexiblere Methoden, um Backup-Fenster einzuhalten und Restore-Zeiten zu beschleunigen.

Das wichtige Thema der Wiederherstellung im Katastrophenfall (Disaster Recovery) darf dabei ebenfalls nicht aus den Augen verloren werden um eine Erhöhung der operationellen und Geschäftsrisiken zu vermeiden.

Der Leitfaden »Backup / Recovery / Disaster Recovery« (Data Protection and Recovery, DP&R) soll sowohl eine Übersicht zu dem Themengebiet der Datensicherung und Wiederherstellung geben als auch die Ende 2016 neuesten Trends aufzeigen. Er soll den zuständigen Funktionen in den Unternehmen als Unterstützung und Wegweiser dienen. Die verwendeten Fachbegriffe wurden im Kapitel 1.5 beschrieben.

Die sich stetig verändernden Anforderungen zum Thema vertiefen die Autoren im Kapitel 2. Unter anderem wird dabei auf die Primärstorage Trends und auf die gesetzlichen Anforderungen bei einer Datensicherung eingegangen.

In Kapitel 3 wird auf die wesentlichen Entwicklungen und Trends von DP&R im Überblick eingegangen.

Die aktuellen Trends werden im Kapitel 4 (DP&R Software/Methoden) und Kapitel 5 (DP&R Hardware) tiefer erläutert. Beispielsweise geht Kapitel 4 auf die Datensicherung von In-Memory Datenbanken, »Backup in the Cloud« und »Software Defined Data Protection« näher ein. In Kapitel 5 werden Unterschiede und Einsatzgebiete der verschiedenen Backup Medien (wie Tape, Disk, Deduplication-Appliances und sonstiger PBBAs) erläutert.

Auch beim Einsatz der neuen Software- und Hardware-Trends/Lösungen bleibt es weiterhin wichtig, die Datensicherung als Ganzes zu sehen und konzeptionell sinnvoll mit den anderen IT-Prozessen zu verbinden. Veränderungen der IT-Landschaft oder auch bei der Nutzung der IT können zusätzliche Anforderungen an die DP&R-Infrastruktur in Richtung Funktionalität, Kapazität und Performance nach sich ziehen. Daher haben die Autoren Hinweise zum Aufbau und Verbesserung von eigenen DP&R Konzepten im Kapitel 6 zusammengefasst. Neben Themen wie Change Management ist ein Beispiel für ein DP&R Betriebskonzept und Tipps zum Disaster-Recovery-Handbuch enthalten.

## Was verstehen wir unter »Backup / Restore / Disaster Recovery«

Die Fachbegriffe Backup, Restore und Disaster Recovery gehören alle zum Themengebiet Data Protection and Recovery, kurz auch DP&R genannt.

Backup beschreibt dabei die Sicherung der Daten, also das Festhalten von Datenzuständen zum Zwecke eines evtl. notwendigen späteren Wiederherstellens (Restore). Das primäre Ziel einer Datensicherung ist ein Unternehmen vor dem Verlust seiner Daten zu bewahren, in dem diese an eine zweite Lokation kopiert/gesichert werden. Die Anzahl der Sicherungspunkte (einen bis mehrere pro 24h sind üblich) wird über die Recovery Point Objective (RPO) definiert. Backups werden i.d.R. Tage bis Monate aufbewahrt (Retention Time), um auf zurückliegende Daten und Konfigurationen zugreifen zu können. Typischerweise sollte ein Medienbruch und ein sicher getrennter weiterer Brandabschnitt in einer Backup-Kette implementiert werden, um wesentliche Risiken zu minimieren. Dazu werden die Unternehmensdaten auf ein separates Speichermedium kopiert.

Bei der Datenwiederherstellung (dem Restore) geht es darum, unter Verwendung der vorhandenen Sicherungen (Backups) Datenzustände der Vergangenheit wiederherzustellen. Der Restore kann kleine Objekte, ganze Dateien, Datenträger oder gar Systeme umfassen.

Die Recovery umfasst neben dem Restore noch weitere IT-Prozesse, die zur vollständigen Dienst-Wiederherstellung durchgeführt werden müssen. Gerade bei größeren Hardware oder Systemausfällen ist es wichtig zu wissen wie lange die Recovery dauern kann.
Die benötigte Zeitspanne wird als Recovery Time Objective (RTO) bezeichnet.

# 2 Aktuelle Herausforderungen an Backup und Recovery-Konzepte / Lösungen

# 2 Aktuelle Herausforderungen an Backup und Recovery-Konzepte/ Lösungen

Anforderungen an Datensicherungskonzepte verändern sich stetig. Die folgende Sammlung der Hauptherausforderungen für DP&R Umfelder verdeutlicht, wo die Ursachen für die üblichen Probleme liegen und welche Themen die nächsten Jahre durch passende Backup- und Recovery-Lösungen zu meistern sind.

## 2.1 Primärspeicher Trends

Im Primärspeicherbereich, also dem Bereich auf dem die aktiven Daten gespeichert werden, sind die folgenden drei Trends zu beobachten:

### Harddisks (HDD):

Bei den Festplatten ist seit weit über einem Jahrzehnt eine deutliche Entwicklung zu beobachten, bei der die Kapazitäten pro Diskspindel deutlich schneller als deren Geschwindigkeit wachsen. Daraus resultieren immer größere Festplatten, die aber nicht in der gleichen Weise an Geschwindigkeit zu legen.

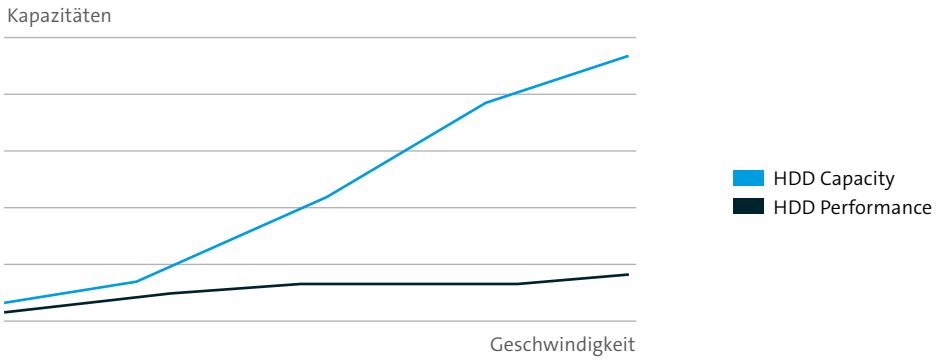



Abbildung 1: Unterschiedliche Entwicklung der Kapazitäten und Geschwindigkeit pro HDD

## Flash (Storage Class Memory):

Flashspeicher in Form von SSDs, Flash-Karten am Storage-Controller und Applikationsserver mit ihren sehr schnellen Zugriffszeiten werden immer mehr genutzt um kürzeste Zugriffszeiten auf die Daten zu ermöglichen. Gemeinsam eingesetzt mit dem immer größeren Festplatten Kapazitäten, kompensieren sie deren langsamere Geschwindigkeit, erlauben aber zeitgleich größere Datenmengen zu speichern.

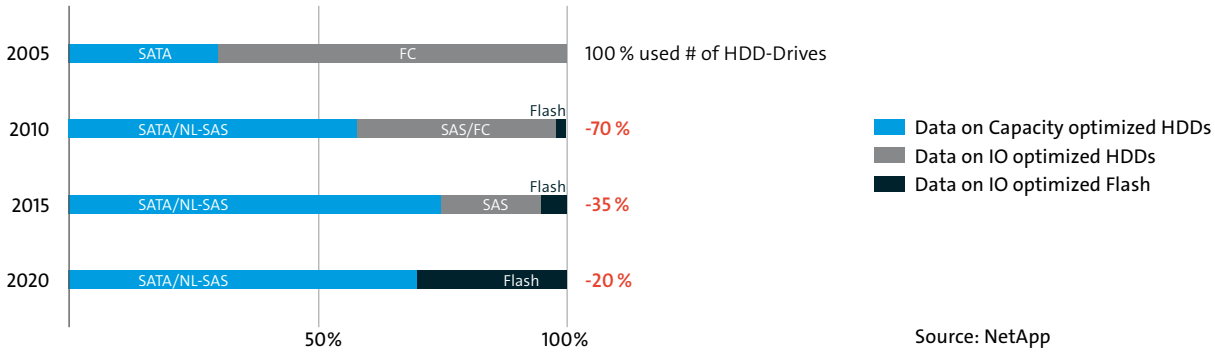



Abbildung 2: Flash Speicher ersetzt IO-optimierte HDDs

## Komprimierung und Deduplizierung:

Ein weiterer Trend im Primärspeicherbreich ist das verdichtete Speichern der Daten. Die Verdichtung erfolgt hierbei durch Komprimierung und / oder Deduplizierung der Daten. Das verdichtete Speichern der Daten hat aber gerade im Backup und Restore Fall Nachteile, da das Lesen der Daten bei der Sicherung und ebenso das Schreiben beim Speichern durch die Komprimierung und / oder Deduplizierung der Daten verlangsamt wird.


Abbildung 3: Vergleich Daten einer Festplatte mit und ohne Komprimierung und Deduplizierung

Um allen drei Primärspeicher-Trends gerecht zu werden, sind B&R (Backup und Recovery) Techniken sinnvoll, die möglichst wenige Daten bewegen müssen. Dazu gehören zum Beispiel sehr granulare incremental-forever Backup-Logiken und sehr granulare differentielle Restores. Gerade beim Restore ganzer Speicherbereiche / Volumes, ist es sehr hilfreich durch Umschalten auf die zuvor eingefrorenen Stände die Daten wiederherzustellen.

## 2.2 Die Anzahl unstrukturierter Dateien wächst

In der heutigen Zeit generieren und speichern Unternehmen immer mehr Daten. Insofern viele Millionen von Dateien (Files) vorhanden sind, wird jedes Backup mit dateibasiertem Verfahren zur Herausforderung. In solchen Fällen empfiehlt sich eine Backup-Logik, welche nicht auf Datei-Ebene sichert. Jedoch bleibt es beim Einsatz solcher Verfahren weiterhin wichtig, einzelne Dateien wiederherstellen zu können.

## 2.3 Die Datenbankgrößen wachsen

Neben dem Wachstum der unstrukturierten Daten werden aber auch immer mehr Daten in strukturierter Form in Datenbanken gespeichert. Dies hat zur Folge, dass die Datenbanken immer größer werden. Dadurch werden auch die Anforderungen an B&R immer weiter erhöht und vor allem die Laufzeiten bei der Datenbanksicherung aufgrund des immer höheren IO-Aufwandes zum Problem. Reduzierte IOs und weniger Systemlast für B&R-Prozesse, als auch mehr Recovery-Points pro 24h (für die Beschleunigung einer Roll-Forward-Recovery) wären hilfreich.

## 2.4 B&R kleiner Niederlassungen und zwischen großen Standorten

Bei den Datensicherungskonzepten für kleinere Niederlassungen ist ein Trend erkennbar, bei dem die Absicherung der lokalen Backups nicht mehr durch eine Kopie der Daten auf Tape erfolgt, sondern viel mehr durch eine Übertragung der Backupdaten in einen zentralen Standort oder zu einem Cloud-Speicher. Ähnlich ist es bei der Absicherung zwischen zwei größeren Standorten. Im Allgemeinen wird dadurch auch eine bessere DR-Readiness erreicht, unter anderem durch frühzeitiges Speichern der Backups in ein sicher entferntes Rechenzentrum (RZ). Eine extrem reduzierte WAN-Belastung durch B&R ist dafür notwendig und hilfreich. Des Weiteren sollten die Backups in einem Format vorliegen, welches im Disaster Recovery Falle schnell aktivierbar ist.

## 2.5 Virtualisierung von Servern und Datenspeichern

Die Virtualisierung von Applikationsservern ist zum Standard geworden. Die zu sichernden Virtuellen Maschinen (VMs) nebst virtualisierter Backup-Targets wechseln zunehmend dynamischer die Lokation, was es erschwert die klassischen 1:1 Beziehungen zwischen lokalem Backup Server und lokalem Backup Client herzustellen.

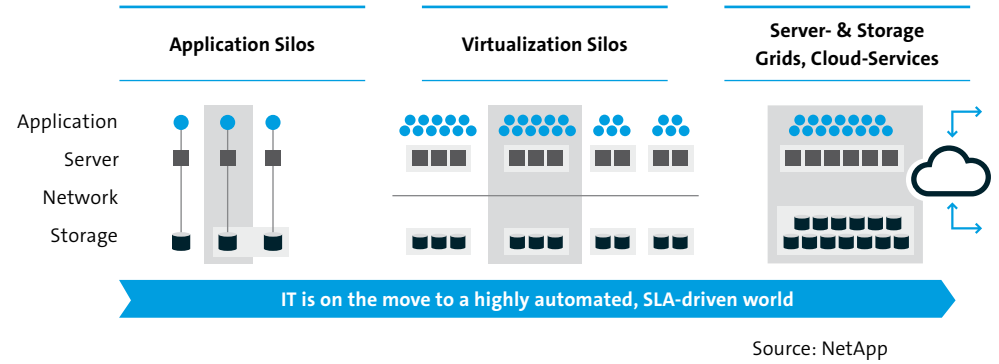



Abbildung 4: Server- und Datenspeicher-Virtualisierung

Reduzierte IOs für B&R und ein uneingeschränkter Applikationskomfort für Restores aus Hypervisor-Level Backups wären wünschenswert. Ebenso die Flexibilität mit sich ändernden Lokationen transparent klar zu kommen.

## 2.6 Automatisierungs- und Cloud-Fähigkeit (DPaaS und DRaaS)

Um die steigenden Anforderungen an DP&R erfolgreich umzusetzen und zu managen, ist ein immer höherer Automatisierungsgrad von DP&R Prozessen erforderlich. Backup-Verantwortliche sollten wie ein Dirigent in die Lage versetzt werden, Backup-Prozesse über zentrale Vorgaben zu orchestrieren. Die eigentliche Ausführung und Überwachung sollte dagegen immer mehr regelbasiert und automatisiert durchgeführt werden. Durch diese Fähigkeiten wird eine Integration von typischen Cloud-Diensten wie DPaaS (Data Protection as a Service) und DRaaS (Disaster Recovery as a Service), sowie Cloud-Speicher für Backupdaten vereinfacht. Aktuelle Datensicherungskonzepte sollten also einen hohen Automatisierungsgrad enthalten und Cloud-Ready sein.

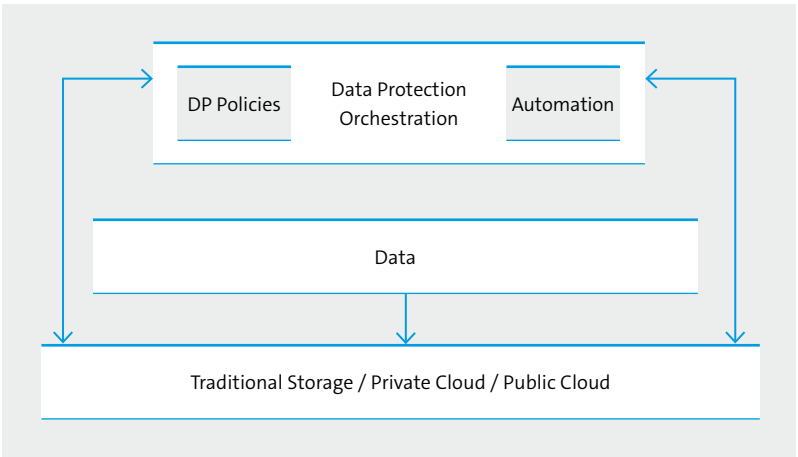



Abbildung 5: DP Orchestrierung mit Automatisierung & Cloud-Unterstützung

## 2.7 Die steigende Abhängigkeit von der IT führt zu erhöhten Ausfallrisiken

Die Kosten von Datenverlusten und der Nichtverfügbarkeit von IT-Services werden immer höher. Neben verbesserter Hochverfügbarkeit der primären Systeme sind die B&R SLAs (RPO, RTO) und die DR-Readiness zu optimieren, um Kernprozesse der Unternehmen hochverfügbar und störungsarm zu halten.

# 3 Trends bei den DP&R-Verfahren

# 3 Trends bei den DP&R-Verfahren

In diesem Kapitel wird im Überblick auf die wesentlichen Entwicklungen und Trends bei den Verfahren zu Backup, Recovery und Disaster-Recovery eingegangen. Oft wird man verschiedene Methoden für Data Protection und Recovery (DP&R) kombinieren, um alle Anforderungen zu erfüllen.

## 3.1 Trend zu weniger Datenbewegung für DP&R

Wie in der Einleitung erwähnt, speichern und nutzen Unternehmen mehr Daten als je zuvor. Damit DP&R Prozesse sich nicht verschlechtern, sondern effizienter und schneller werden, gab es viele Weiterentwicklungen, welche die Menge der zu transportierenden Daten beim Backup / Restore reduzieren.

Die wesentlichen Entwicklungen und Trends bei den DP&R Verfahren werden nachfolgend in fünf Generationen (nach dem Kriterium Reduktionsfortschritt von Datenbewegungen) unterteilt. D. h. in der ersten Generation werden noch sehr viele und mit jeder folgenden Generation deutlich weniger Daten für DP&R bewegt.

Natürlich könnte man DP&R Techniken / Verfahren auch anders kategorisieren. Der Bitkom Expertenkreis entschied sich für das Evolutionsmodell, welches in folgender Grafik als Übersicht dargestellt wird. Die Details und Unterschiede zu den einzelnen Generationen sind in den nachfolgenden Kapiteln beschrieben.

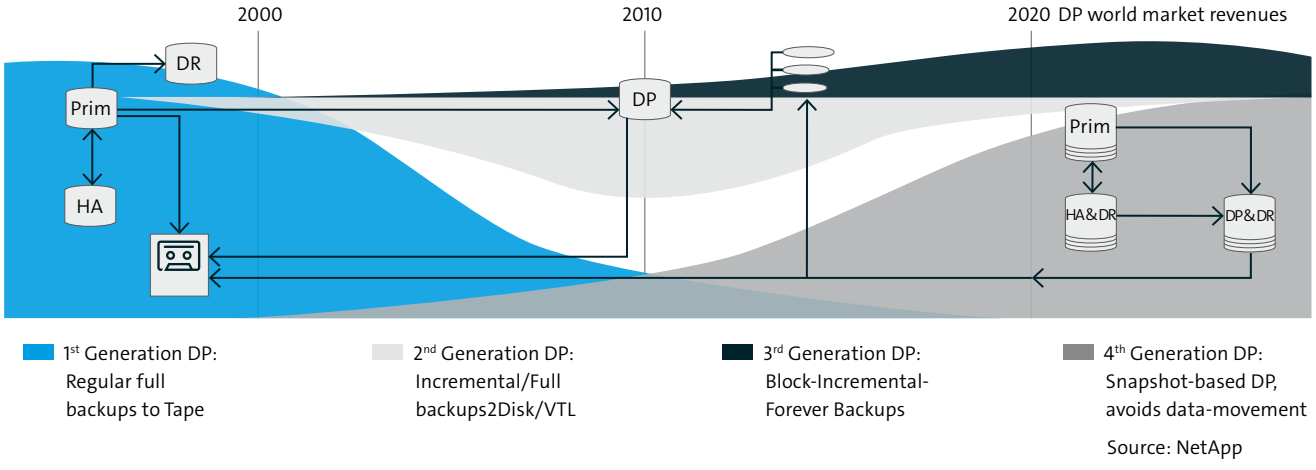
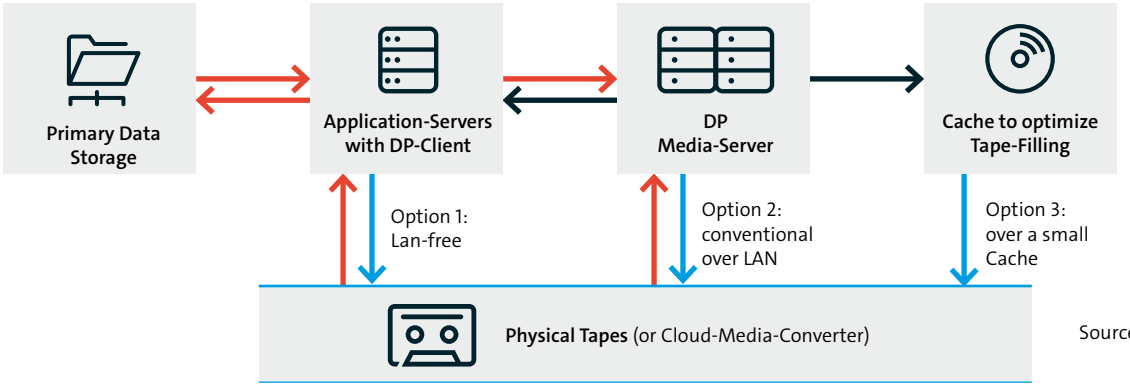



Abbildung 6: Übersicht DP Evolutionsmodell

In der Grafik werden die bisherigen und erwarteten Veränderungen (der Weltmarkt-Investitionen aller Kunden) über einen langen Zeitraum von ca. 40 Jahren grob abgeschätzt.

## 3.2 »1st Generation DP&R«: Full Backup – Backup2Tape

So lange Full-Backups die Regel sind (ggf. ergänzt um Differential-Backups = Zuwachs-Sicherungen), sprechen wir von 1st Generation DP&R. Besonders häufig verwendet man dafür das Backup-Medium Tape. Tape erfordert wegen seinen sehr langen Direktzugriffszeiten regelmäßig Full-Backups, weil mehrere Incremental-Backups extrem lange Restore-Zeiten nach sich ziehen würden. Tape ist daher nur für DP&R Generation 1 als primäres Backup-Medium sinnvoll.




Source: NetApp

Abbildung 7: Data to be transported with 1st Gen. backups to tape or to restore from tape

Bei der Option 3 von 1st Generation DP&R ist die Größe des Disk/Flash-Cache klein ausgelegt. Er dient somit nicht der Restore-Beschleunigung, sondern nur dem optimierten Befüllen der Tape Medien. Kommt ein solcher »Disk-Cache« zum Einsatz, liegt zwar technisch für den Backup-Prozess ein »Backup to Disk to Tape« (Backup2Disk2Tape) Verfahren vor, Restores erfordern hier aber fast immer Tape-Zugriffe – daher ist hier der Zwang zu regelmäßigen Full-Backups weiter gegeben.

**Information**

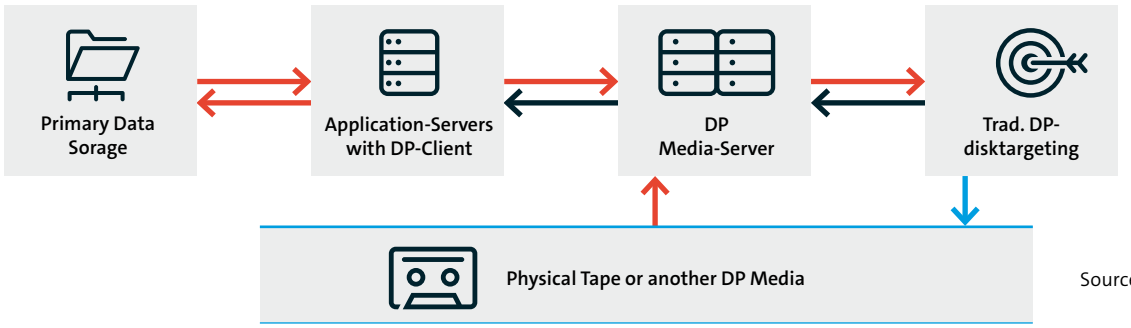
Generelle Zeichenerklärung für die Grafiken in 3.2 bis 3.5:

- Die Pfeildicke symbolisiert die zu transportierende Datenmenge für die Backup-/Restore-Prozesse (dünner Pfeil: wenig Daten zu übertragen, dicker Pfeil: viele Daten zu übertragen).
- Die Pfeilfarbe symbolisiert, ob dieser Teilschritt des Backup- oder Restore-Prozesses typischerweise einen Engpass (rot), keinen Engpass (blau) oder einen Mittelwert davon (schwarz) darstellt.

## 3.3 »2nd Generation DP&R«: häufige Incremental Backups – Backup2Disk

Zwar werden hier immer noch gelegentlich Full-Backups notwendig, aber Incremental-Backups sind die Regel. In der Summe ist somit ab 2nd Generation DP&R eine deutliche Reduktion der Backup-Datenmenge möglich. Dies setzt allerdings ein Backup-Medium voraus, welches relativ schnelle Direktzugriffe erlaubt – Disk ist hierfür sehr üblich. Damit Restores nach Incremental Backups schnell ausführbar sind, müssen zumindest die Incremental-Backups über eine ganze Reihe von Backup-Generationen hinweg auf Disk vorgehalten werden.

Mehr Backups und eine höhere Parallelität beim Restore werden möglich.
Weitere Details zu Incremental-Backups sind bei den Fachbegriffen beschrieben.

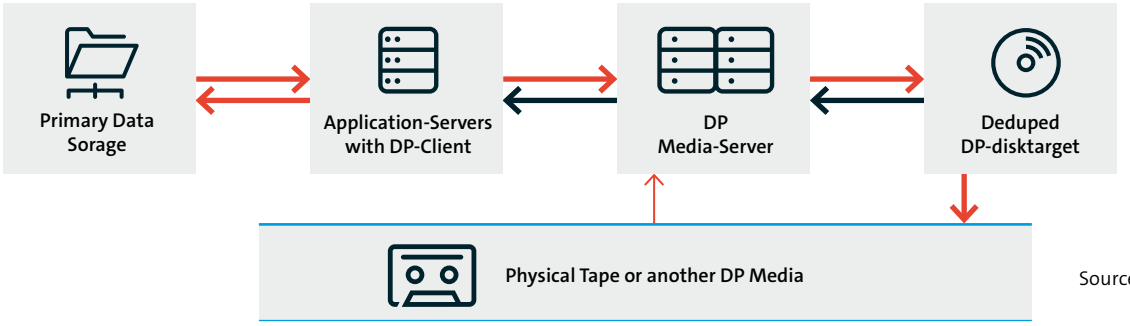



Source: NetApp

Abbildung 8: Data to be transported with 2nd Gen. DP&R with traditional disktargets

Diskbasierte Backup-Medien können unverdichtet oder nur mit Komprimierung betrieben werden (siehe obige Grafik), dies lässt aufgrund des großen Kapazitätsbedarfs nur ein bis wenige Tage Backup-Speicherung auf Disk zu. Ältere Backup-Generationen werden meistens auf einem Tape basierten Backup Medium aufbewahrt (Backup to Disk to Tape). Um den disk-basierten Speicher optimaler zu nutzen, wird teilweise eine Beschränkung der Disk-Medien auf alle Incremental- und kleine Full-Backups vorgenommen.

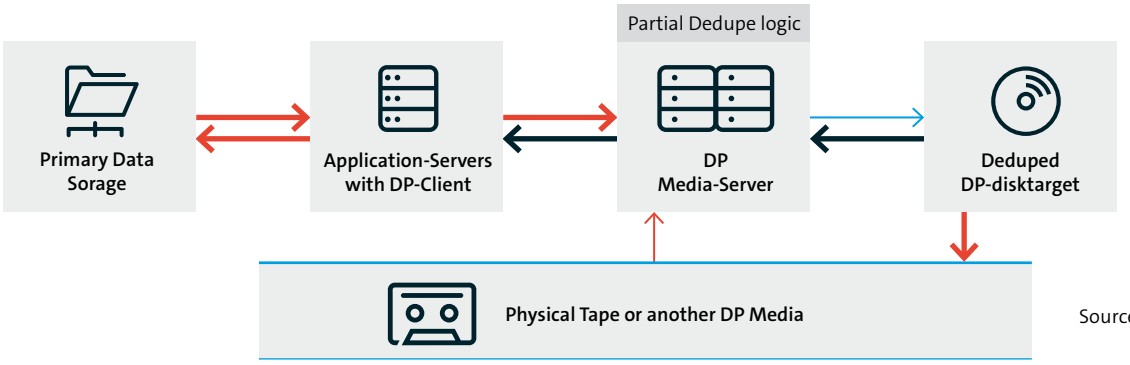
Mit dem Einsatz von Deduplication-Verfahren für Backups (weitergehend beschrieben in Kapitel 5.3), können alle 2nd Generation Backups über mehrere Wochen bis hin zu Monaten auf Disk-Medien vorgehalten werden. Im nachfolgenden Abschnitt werden die verschiedenen eingesetzten Deduplication-Verfahren näher erläutert.




Source: NetApp

Abbildung 9: Data to be transported with 2nd Gen. DP&R by a PBBA with Target Deduplication

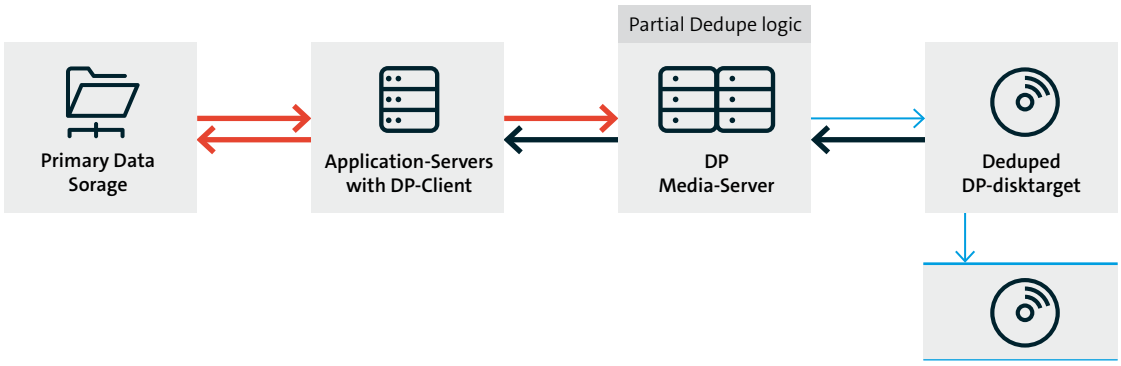
Viele Backup-Software-Hersteller haben Target Deduplication bereits integriert. Alternativ kann für fast jede Backup-Software eine Dedupe-fähige Purpose Build Backup Appliances (PBBAs) eingesetzt werden (mehr zu PBBAs unter 5.5).




Source: NetApp

Abbildung 10: Data to be transported with 2nd Gen. DP&R by a PBBA target with distributed Dedupe-Logic

Manche Backup-Software kann mit bestimmten PBBAs eine verteilte Deduplication-Logik anwenden (siehe Kapitel 5.5.1).




Source: NetApp

Abbildung 11: Data to be transported with 2nd Gen. DP&R by a PBBA with Deduped Replication

Nach dem Deduplication können Backups über Deduped-Replication verdichtet in andere Rechenzentren verbracht werden (siehe Kapitel 5.5.1).

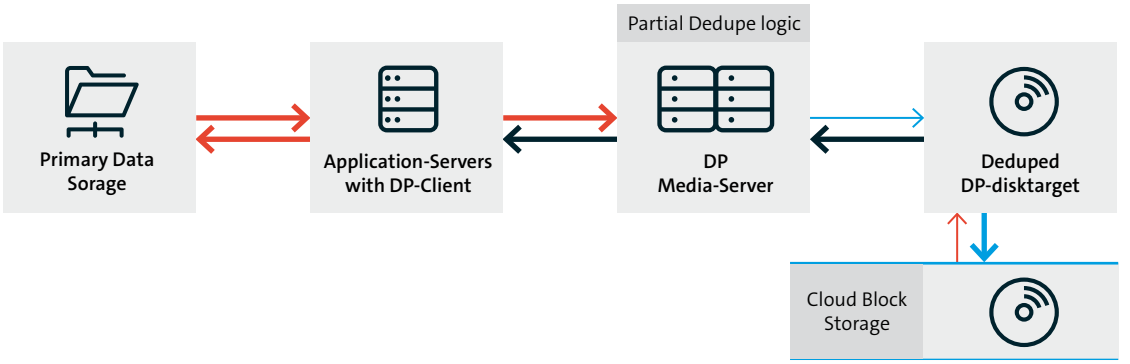



Abbildung 12: Data to be transported with 2nd Gen. DP&R by a PBBA cache with Cloud-Storage storing

Ein Deduped Disk-Cache in Verbindung mit günstigem Cloud-Storage kann die Gesamtkosten weiter reduzieren und teilweise Tape unterbieten (siehe Kapitel 5.5.4).

## 3.4 »3rd Generation DP&R«: Incremental Forever Backup

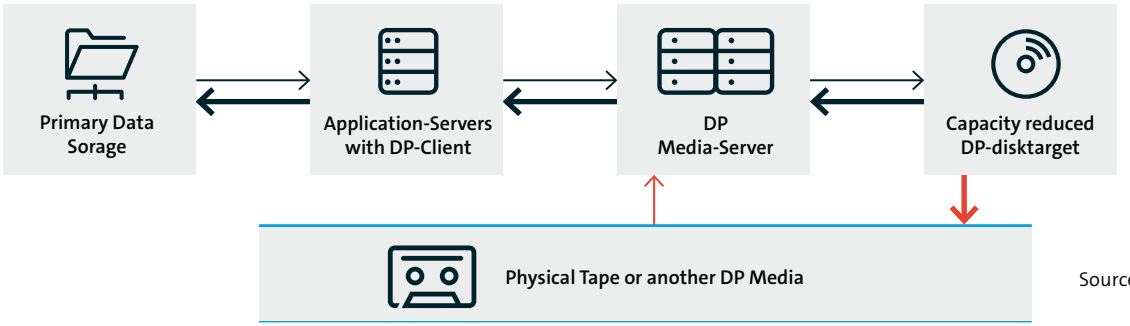
3rd Generation DP&R ist durch einen einzigen Full-Backup zu Beginn gekennzeichnet, danach erfolgen auf Dauer nur noch Incremental-Backups. Es gibt mehrere Verfahren, dies zu erreichen:

- Die Ermittlung der geänderten Dateien erfolgt über »Last Modified Timestamp« oder anderen Datei-Attributen. Dies reduziert die Datenmenge aber maximal auf Datei-Ebene, was für große Objekte (wie Datenbankfiles) nicht effizient ist.

- Die Ermittlung der Differenzblöcke kann über Changed Block Tracking oder über Clientside-Deduplication Verfahren erfolgen. Beim Clientside-Deduplication ist zu beachten, dass es ein weniger effektives lokales Full-Lesen vor dem Transport bedingen kann, sofern kein Changed Block Tracking vorausging.

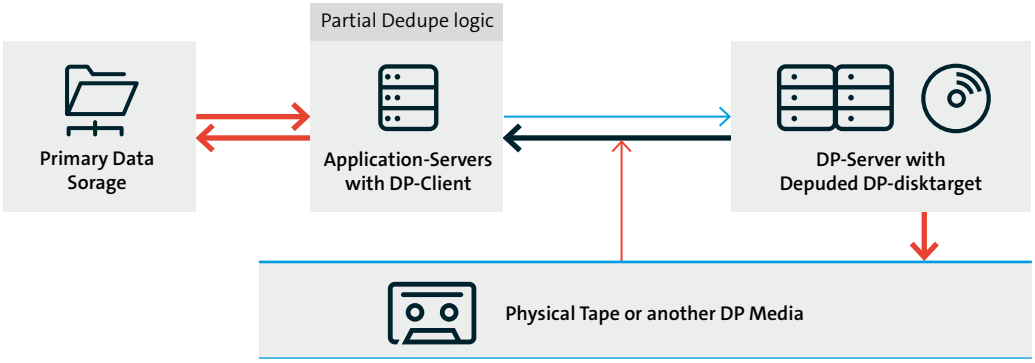
- Teilweise wird dann in der Folge aus den Incremental-Forever Backups ein synthetischer Full-Backup erzeugt. Dies kann über eine DB-Logik, eine Backup-Server Logik oder eine Schnittstelle zu einer PBBA erfolgen, welche durch eine Backup-Software gesteuert wird.

3rd Generation Backups skalieren meist besser als 2nd Generation Backups, da nur die Datenveränderungen seit dem letzten Backup transportiert werden müssen. Beim Restore sind teilweise Laufzeitverschlechterungen gegenüber 2nd Generation Restores gegeben, vor allem weil verstärkt Random-IOs für große Restores anfallen.




Source: NetApp

Abbildung 13: Data to be transported with 3rd Gen. DP&R by Blocklevel-Incremental-Forever

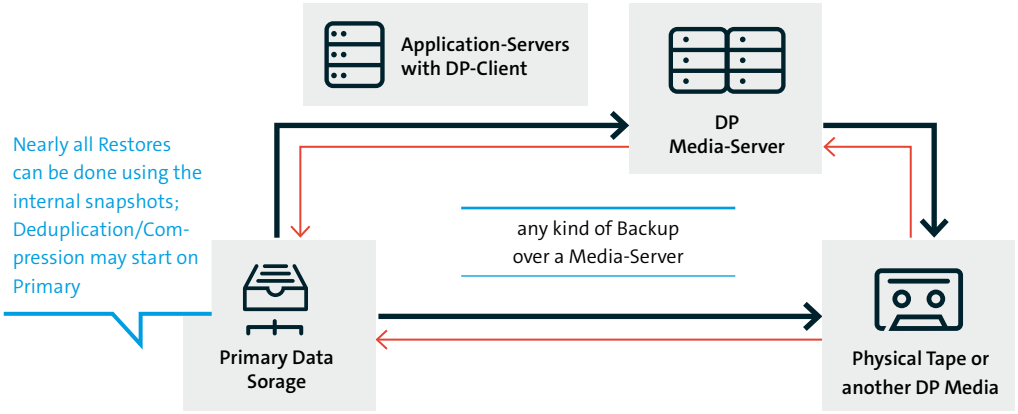



Source: NetApp

Abbildung 14: Data to be transported with 3rd Gen. DP&R by Client site Deduplication

## 3.5 »4th Generation DP&R«: Snapshot-basiertes DP&R

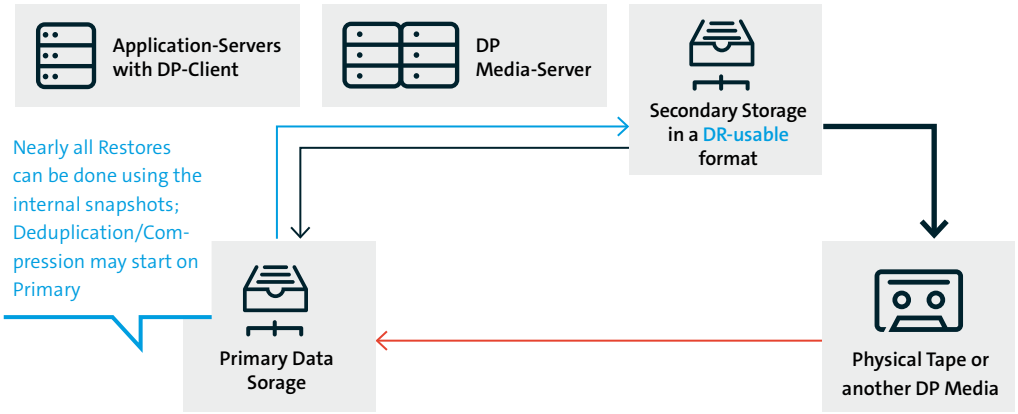
4th Generation DP&R zeichnet sich dadurch aus, dass die Veränderungen und die aktiven Daten zusammen gespeichert werden. Beim Backup wird das bestehende Datenkonstrukt per integrierter Snapshot-Technik sehr schnell eingefroren. Auf jeden gehaltenen Snapshot-Stand kann man bei Restore-Anforderungen sehr schnell zugreifen oder diesen neu aktivieren. Synchrone Spiegel der Primär-Daten, sowie asynchrone Replikationen bzw. ein optionales Tape-Backup sind übliche Ergänzungstechniken. Gegenüber 3rd Generation DP&R werden weitere Verbesserungen beim Backup erreicht, da teilweise keine Daten für die Snapshot-Erstellung bewegt werden. In noch größerem Maße werden aber Verbesserungen beim Restore und bei DR erzielt, da auch für große Restores teilweise keine Daten bewegt werden müssen. Mehr dazu siehe Kapitel 5.4.




Source: NetApp

Abbildung 15: Data to be transported with 4th Gen. DP&R Array Snapshot with Tape-backup

Primärdaten-Snapshots alleine bieten zwar sehr effiziente Restore-Möglichkeiten, aber benötigen zum Schutz vor dem Untergang des Primärdatensystems (auf dem ja auch die Snapshots gespeichert sind) Backups in einen anderen Brandabschnitt. Dafür können andere Backup-Methoden oder Tape-Backups ergänzt werden, welche allerdings dann zeitverzögert die hohen Lasten von 1st, 2nd oder 3rd Generation DP&R erzeugen.




Source: NetApp

Abbildung 16: Data to be transported with 4th Gen. DP&R Array Snapshot with Replication & Tape Backup

Asynchrone Replikationen auf beliebig weit entfernte andere Rechenzentren sind eine bei 4th Generation DP&R oft ergänzte und effektive Technik. Dies kann auch nachfolgende Backups auf andere Medien (wie Tape) optimieren.

Bei Backup-Aufbewahrungsfristen von Wochen bis Monaten kann hier auch ein Verzicht von Backups der Secondary Storage Snapshots nach Risikoabwägung vorgenommen werden – dann arbeitet man nur noch mit hocheffizienten 4th Generation DP&R Techniken.

## 3.6 »5th Generation DP&R«: Objectstores mit Self-Protecting-Storage-Verfahren

Für geeignete Daten (vor allem unstrukturierte) können die immer breiter aufkommenden Objectstore-Techniken einen weiteren Backup- und Recovery Fortschritt darstellen. Die B&R Prozesse sind hier in die Systeme integriert und noch besser für sehr große Datenmengen und sehr viele Objekte geeignet (»Self Protecting Storage«).

Über die Verteilung der Kopien auf verschiedene Brandabschnitte werden die Datensicherung und Wiederherstellung der Datenobjekte intern mit abdeckt. Dadurch ist auch die Außenstellen-Backup/Recovery Problematik für diese Daten i.d.R gelöst bzw. meist aufgrund der hohen Datenmenge kein ergänzendes Backup mehr sinnvoll durchführbar. Weiterhin sinnvoll kann es jedoch sein, ein Backup der Objectstore-Metadaten und -Software durchzuführen, um Restrisiken zu vermindern.

Objectstores bieten immer eine Objektschnittstelle (wie HTTPS, Webdav, OpenStack Swift, S3).

Die teilweise ergänzend gebotenen Legacy-Schnittstellen wie CIFS und NFS können als Brückentechnologie benützt werden, um Objekt-Zugriffe für geeignete Daten zu ermöglichen.

Die Integration der Objectstores in bestehende Anwendungen ist oft noch nicht weit fortgeschritten (teilweise werden Objectstores als HSM-Speicher verwendet) – eigentlich wäre es das Optimum, wenn man die primären Daten sofort und ausschließlich im Objectstore speichert.

Wie bei Archivsystemen muss jede Version eines Objekts bei jeder Veränderung neu gespeichert und nach definierten Regeln auf verschiedene Brandabschnitte verteilt und selbstheilend gespeichert werden. Auch ein Tape-Layer oder Cloud-Speicher-Layer (für einen Teil der Kopien) ist teilweise möglich.

Da ein Objectstore die Datensicherung beinhaltet, muss dieser intern sehr ähnliche Problematiken lösen wie Backup-Systeme traditioneller Art (z. B. Deduplication zur Effizienzsteigerung bei WAN-Replication einsetzen, oder Snapshot-based arbeiten; und eine sehr hohe Zuverlässigkeit der Gesamtfunktionalität inklusive DP&R bieten). Ob und ab wann hier genügend Fortschritte erzielt sind, dass diese Technik als breit anwendbares »5th Generation DP&R« einzustufen ist, bleibt abzuwarten.

Zumindest dürften Objectstore-Techniken als Archivspeicher der Zukunft eine große Rolle spielen. Auf die Abgrenzung zwischen Archivierung und B&R wird im Kapitel 4.5 eingegangen.

Objectstores können auch als Backup-Medium für Backup2Disk-Verfahren eingesetzt werden. Für die Laptop und Desktop Backup Problematik gibt es teilweise eine Replizierungslogik, welche eine Kopie der Dateien bidirektional mit dem Objectstore austauscht.

# 4 DP&R-Software, -Methoden und deren Trends

# 4 DP&R-Software, -Methoden und deren Trends

## 4.1 Trends für DP&R von relationalen DBs

Um die Problematik der wachsenden Datenmengen bei den Datenbanksicherungen zu begegnen, haben sich verschiedene, oft grundsätzlich unterschiedliche Methoden entwickelt. Diese lassen sich generell in zwei Gruppen einordnen:

- Spezielle Datensicherungstools der jeweiligen Datenbanken (bzw. Nutzung derer APIs)
- Sonstige User Managed Backups (ohne Nutzung der DB-Hersteller-Logik)

Die Sicherung von Datenbanken ist eine wesentlich komplexere Aufgabe als die Sicherung von Dateien oder Filesystemen. Datenbanken sind Real-Time Systeme bei denen ein großer Teil der Datenverarbeitung im RAM-Speicher und in verschiedenen Filetypen erfolgt. Letztere sind miteinander logisch verbunden, voneinander abhängig und müssen bei einer Sicherung miteinander synchronisiert werden. Bei Backup-Lösungen ohne DB-Integration, welche diese Abhängigkeiten bei Online-Backups nicht ausreichend berücksichtigen und die Datenbankteile nur als Dateien behandeln, besteht die Gefahr, dass die Konsistenz dieser Datenbankobjekte gebrochen wird und die Wiederherstellbarkeit der ganzen Datenbank deswegen scheitert.

Im Folgenden werden gängige Verfahren zur Sicherung bzw. Wiederherstellung von relationalen Datenbanken mit ihren Vor- und Nachteilen genannt:

### Voll- und Inkrementelle Sicherungen der DB (DP&R Generation 2):

Alle DB-Hersteller unterstützen klassische Full-Backups.

Die meisten der verbreiteten DB-Hersteller unterstützen ergänzend Block-Incremental-Backups.

Bei relativ hohen Änderungsraten und vielen Incrementals kann die Recovery-Zeit der Datenbankfiles aufgrund der langen Logreplay-Zeiträume inakzeptabel lang werden. Daher bieten wenige DB-Hersteller Incremental-Forever Lösungen an, bei denen allerdings zwischendurch ein Synthetic Full-Backup erzeugt wird (z. B. über eine PBBA, siehe Kapitel 5.5). Die meisten Anwender werden jedoch gelegentlich ein echtes Full-Backup der DB (z. B. wöchentlich) einstreuen.

### Snapshot-basierende Sicherungstechniken für Datenbanken (DP&R Generation 4):

Sowohl das Sichern als auch der Restore kann durch Anwendung von Snapshots sehr beschleunigt werden, da hier meist keine Daten, sondern nur Pointer verändert werden. Der zeitliche Vorteil steigt mit der Größe der DB.

Während Snapshot-basiertes Sichern bzw. Wiederherstellen der DB selbst von den meisten Backup-Software Herstellern unterstützt wird, unterstützen nur sehr wenige das Snapshot-basierte Sichern bzw. Wiederherstellen der DB-Logs (Änderungsaufzeichnungen).

Mehr zu den Prinzipien von Snapshot-basierter Sicherung siehe späteres Kapitel 5.4 »Snapshot Differenzblock-Techniken«.

## Recovery-Verfahren für relationale Datenbanken:

1. Ein reines **Transaction-Rollback** nach unkontrolliertem Beenden der DB

2. Eine **Point-In-Time-Recovery** einer DB: Restore der DB auf einen Sicherungsstand (der könnte Application- oder Crash-consistent sein) und anschließendem Transaction-Rollback

3. Eine **Roll-Forward-Recovery** einer DB (ist verbreitet und üblich): Restore der DB auf einen meist Application-consistent Sicherungszustand. Gefolgt von einem Log-Replay der aufgezeichneten Änderungen und anschließendem Transaction Rollback.

   - Dazu ist es Voraussetzung, dass das Änderungs-Log der DB regelmäßig per Log-Truncation abgesplittet wird und am besten mindestens eine Kopie in einem zweiten Brandabschnitt erzeugt wird.

   - Damit lässt sich eine DB auf den jüngsten oder einen bestimmten Zeitpunkt bringen, indem alle zwischenzeitlichen Änderungen seit dem letzten Backup aus den Log-Files neu eingespielt werden.

   - Häufige Backups (viele Recoverypoints) der DB sind wünschenswert, denn diese verkürzen der Log-Replay Zeit erheblich.

4. Nutzung einer vorgehaltenen **Schattendatenbank**: Wird eine Schattendatenbank vorgehalten, in welche mit definiertem Zeitversatz (von z. B. 4h) die Änderungen per übertragenen DB-Logs eingespielt werden, kann dies auch für eine DB-Recovery genutzt werden. Diese ist jedoch nur innerhalb des eingestellten Zeitfensters anwendbar. Da dazu auch eine hohe Automatisierung für Failover bzw. Failback-Prozesse notwendig ist und das Bereitstellen von Ersatz-Rechenleistung durch Virtualisierung vereinfacht wurde, ist die Verwendung dieser Option rückläufig.

Besonders alle Recovery-Methoden, welche mit einem Wiedereinspielen von DB-Logs arbeiten, können als »nearly continuously Dataprotection« Methoden eingestuft werden, sofern das DB-Log sichern sehr häufig erfolgt – aber auch häufige Snapshots der DB kommen dem Ziel nahe.

## 4.2 DP&R von In-Memory Datenbanken

InMemory Datenbanken verbreiten sich zunehmend im heutigen Rechenzentrum. Diese unterscheiden sich von klassischen Datenbank-Systemen dadurch, dass die komplette Datenbank im Arbeitsspeicher des Servers gehalten wird.

Aus diesem Grund wird üblicherweise der Inhalt oder das neue Änderungs-Delta der Datenbank regelmäßig auf nicht flüchtige Massenspeicher geschrieben.

Wird eine InMemory DB nur eingesetzt um Analysen durchführen zu können, stellt sich aus Backupsicht die Frage, ob diese überhaupt in ein Backup einbezogen werden muss, da hier nur eine wiederherstellbare Kopie von Original-Daten gehalten wird.

Ändert sich eine InMemory DB regelmäßig, muss diese in die Backup Strategie einbezogen werden. Hier zeichnen sich folgende Ansätze ab:

- Die DB-Hersteller liefern oft eine Standardoption »Schreiben auf Disk-Files« mit.
- Die meisten InMemory DB´s bieten API´s für Backup Agenten an.
  Damit lässt sich eine InMemory DB in klassische Backupkonzepte integrieren, sofern die DB-API (Application Program Interface) unterstützt wird.
- Als Backup-Medium können Storage-Snapshots erwogen werden, vor allem, wenn die API granulare Änderungs-Deltas sendet.
- Idealerweise sollte auch ein Reporting bzw. Monitoring der Backupprozesse möglich sein.

## 4.3 Asynchrone Replikation der Backups

Aus den Trends zu häufigeren Datensicherungen pro 24h (RPOs) ergibt sich ein Trend zur asynchronen Daten-Replikation auf Datei- oder Blockebene. Die Voraussetzung für die Einführung von Lösungen zur asynchronen Spiegelung bzw. asynchronen Replikation von Daten, ist in allen Fällen der Einsatz von Direktzugriffsmedien (üblicherweise Disk) als Sicherungsmedium. Aktuelle Lösungen bieten darüber hinaus intelligente Datenreduktionsfunktionalitäten (mindestens Komprimierung, meistens ergänzend Daten-Deduplizierung oder differentielle Snapshots) um die benötigte Bandbreite für die Replikation der Backups so gering wie möglich zu halten.

Trotz dieser Datenverdichtungen muss die Netzwerkarchitektur (FC oder IP basierend, auch übers Internet) ausreichend dimensioniert werden.

## 4.4 B&R SLAs

Die steigende Abhängigkeit der Unternehmen von IT gestützten Diensten führt oft zur Erkenntnis, dass die Verfügbarkeit dieser Dienste und der Schutz vor Datenverlust weiter zu erhöhen ist. Dies kann erfordern, langjährig bewährte Backup-Strategien bzw. Verfahren in Frage zu stellen und mit neuen Verfahren verbesserte SLAs zu ermöglichen.

Für externe IT-Dienstleister waren SLAs mit definierten Kennzahlen schon lange selbstverständlich. Immer mehr innerbetriebliche IT-Abteilungen stellen sich als Dienstleister gegenüber Ihren Fachbereichen auf und bieten ebenfalls Service-Levels an; teilweise in Konkurrenz zu externen Anbietern oder als interne Zielvereinbarung zwischen dem IT- und Fachbereich.

Folgende Inhalte und Kennzahlen sind typisch für SLAs – ggf. in verschiedene SLA-Klassen (wie »Gold«, »Silber« und »Bronze« unterteilt) – und jeweils unterschieden zwischen üblicher Recovery und im Falle einer Disaster-Recovery:

- Monatliche oder Jährliche Gesamtverfügbarkeits-Rate der Anwendung in %
  - dies hat auch Auswirkung auf die Backup- und Recovery Prozesse, sowie der SLAs der IT, z. B. die Verfügbarkeit der Backup-und Recovery-Infrastruktur selbst
  - um Logikfehler einzelner Backup-Methoden überbrücken zu können, kann der Einsatz verschiedener Backup-Methoden für die gleichen Daten erwogen werden (Array-Snaphots, Hypervisor-Level Backups von virtuellen Disks und/oder traditionelle logische Backups könnten parallel eingesetzt werden)
- Definition des maximalen zeitlichen Datenverlustes beim Zurücksetzen (hat Auswirkung auf die RPOs)
- Wie lange darf es maximal dauern, bis eine Recovery durchgeführt ist (RTO = Recovery Time Objective)?
- Wer darf Zugriff auf unverschlüsselte Backupdaten bekommen?

## 4.5 Aufbewahrungsfristen (Expiration), Archivierung vs. »DP Archival«

Aufbewahrungsfristen für Daten lassen sich grob in zwei Kategorien einteilen:

a. gesetzlich vorgeschriebene Aufbewahrungsfristen (siehe Anlage »Rechtliche Anforderungen«)
b. selbstdefinierte Aufbewahrungsfristen

Jeder Kunde hat für sich zu entscheiden, ob er für die mehrjährige Langfristhaltung dieser Daten Archivsysteme oder Backupsysteme benützt, bzw. Backups als »doppelter Boden« neben der Archivierung gehalten werden.

Besonders beim langjährigen Halten von Backups sollte man das Risiko der Nichtinterpretierbarkeit der logischen Dateninhalte abwägen, denn die gesicherten technischen Container (LUNs, DB, Office-Files usw.) garantieren alleine nicht mehr die Lesbarkeit (OS, Software usw. aus der damaligen Systemumgebung lassen sich evtl. in zukünftigen Umgebungen nicht mehr betreiben).

Am Markt ist ein leichter Trend zur Nutzung von Archivierung zu erkennen. Sofern Archivierung für diese Zwecke benützt wird, werden die Vorhaltezeiten von Backups typischerweise deutlich verkürzt (auf Wochen, Monate oder maximal ein Jahr).

Aufgrund der Verdichtungstechniken von Disk und immer günstigerem Preis pro TB ist ein leichter Trend erkennbar, Daten länger aufzubewahren. Vor allem für Daten die älter als ein Jahr sind und Zugriffszeiten von mehreren Minuten akzeptabel sind, erscheint Tape weiterhin als ein bevorzugtes Medium.

## 4.6 Anzahl von Backup-Kopien

Da die Unternehmen immer mehr von den IT-Daten abhängig sind, ist ein Trend zum erhöhten Schutz vor Datenverlust über die Haltung von mehr Datenkopien zu beobachten. Zumindest für wichtige Produktionsdaten ist die Einhaltung folgender Regeln erwägenswert:

- Neben den Produktivdaten mindestens zwei Datenkopien halten
- Darauf achten, dass die Kopien insgesamt auf mindestens zwei sicher getrennte Lokationen verteilt sind (dies könnte auch durch Auslagern von Tapes erfolgen)
- Ein Medienbruch gegeben ist (der logische Medienbruch erscheint hier wichtiger als der physische Medienbruch)
- Oft ist eine Verschlüsselung und Weitergabekontrolle zu erwägen – siehe rechtliche Aspekte in der Anlage

## 4.7 RPOs / nearly Continuous / Continuous DP (CDP)

Zumindest bis zum Jahr 2000 war es noch üblich, nur einen Backupstand pro 24 Stunden zu halten. Der Trend geht klar zu deutlich mehr Backupständen in 24 Stunden, bis hin zu kontinuierlicher Datensicherung. Ziel dieser Verbesserungen ist, im Desasterfall deutlich weniger Daten zu verlieren.

### Häufige Backupstände (gute RPOs) über differentielle Snapshots:

Hiermit sind derzeit teilweise bis zu fünf Minuten Abstand zwischen den Backupständen realisierbar, Stündliche Snapshots schon weit verbreitet. Die Tendenz geht zu noch häufigeren Snapshots.

### CDP für relationale DBs:

Relationale DB zeichnen schon seit langem kontinuierlich Ihre Änderungen auf (»Achivelogs« usw.). Diese erlauben eine Recovery zu einer beliebigen Zielsekunde. Das Erzeugen der Log-Files (um diese in andere Brandabschnitte zu verlagern) ist jedoch nur semi-synchron möglich.

CDP für Datenbanken über darauf spezialisierten Backup-Appliances (PBBA) werden im Kapitel »Backup relationaler DB« mitbeschrieben.

### Sonstige CDP Systeme:

Es gibt Verfahren bzw. Systeme, welche die Produktionsdaten asynchron auf (auch weit entfernte) Systeme replizieren.

Andere Systeme bieten auch eine synchrone Replikation an, was allerdings zumindest bei größeren Entfernungen zu Performance-Einbußen am Primärsystem führt.

### Application-Consistency ist bei sehr häufigen Backups meist ein Problem:

Meist ist die Herstellung von Application-Consistency (Applikationskonsistenz) entweder nicht mit den obigen Verfahren integrierbar (die meisten Applikationen unterstützen keine CDP-Schnittstelle). Außerdem ist dieses Herstellen von Application-Consistency mit einem störenden Applications-Overhead verbunden, so dass man es in der Praxis nicht sinnvoll anwenden kann.

Folglich arbeiten die meisten der obigen Verfahren nur Crash-consistent (siehe auch Kapitel 4.9).

## 4.8 Sensitivität der Daten (Schutz der Dateninhalte, Encryption etc)

Die zunehmende globalisierte Vernetzung von Unternehmen und deren genutzter IT-Dienste stellt den Schutz der unternehmenseigenen Daten vor neue Herausforderungen. Dies gilt neben den produktiven Daten auch für davon erstellte Sicherungssätze. Hier ist eine zunehmende Sensitivität wahrzunehmen, auch B&R-Prozesse an heutige Datenschutzanforderungen anzupassen. Dazu gehören Richtlinien, die den Zugriff auf die gesicherten Daten regulieren und protokollieren, als auch die Nutzung von aktuellen Verschlüsselungsmethoden, wie z. B. AES256.

Für eine Verschlüsselung der Backups spricht beim Einsatz von Backup-to-Disk Speichersystemen die Tatsache, dass laufend zugegriffen werden kann; bei Backup auf Tape, dass nach der Entnahme aus der Tape Library beim Transport oder der Lagerung evtl. Dritte unbemerkt Zugriff bekommen oder Medien verschwinden könnten.

Soft- und Hardware-Lösungen aus dem Bereich »Identity und Access Management« können die Zugriffsrichtlinien, Berechtigungsverwaltung und deren Protokollierung unterstützen.

Siehe auch die rechtlichen Aspekte in der Anlage.

## 4.9 Application-Consistency vs. Crash-Consistency

Crash-Consistency: die Write-IO Reihenfolge bleibt 100% erhalten; der Zeitpunkt der Sicherung wird nicht mit der Applikation abgestimmt. Meist wird dies über Snapshot-basierte Verfahren oder Replikationen erreicht, welche in der Lage sind alle Daten innerhalb von Millisekunden »einzufrieren«.

Application-Consistency: Die Applikation ist zum Zeitpunkt der Sicherung entweder beendet oder sie wird über bereitgestellte Verfahren in einen speziellen hotbackup-Modus versetzt. Diese Prozesse werden teilweise als »quiescing« bzw. »unquiescing« bezeichnet und sind zum einen für Backup-Prozesse komplexer in der Anwendung und zum anderen mit teilweise größeren Verzögerungen verbunden.

Daher ist am Weltmarkt ein Trend erkennbar, zunehmend Crash-Consistency-Backups für Recovery-Zwecke zu nutzen. Meist wird dann mit einem Mix aus häufigen crash-consistent Backups und täglichen oder wöchentlichen Application-consistent Backups gearbeitet.

Alle Applikationen, welche nach unplanbaren Ereignissen wie OS-Abstürzen oder Stromausfällen beim Restart wieder auf einen sauberen Stand kommen, werden auch beim Zurücksetzen aus crash-consistent Sicherungsständen kein Problem haben.

Der Vorteil von crash-consistent Backups liegt im stark verminderten System-Overhead, da der Aufwand zum Wechsel in und aus dem Hotbackup-Modus entfällt.

Man sollte darauf achten, dass bei den meisten relationalen Datenbanken crash-consistent Backups nicht für Roll-Forward-Recoveries benützt werden können (Stand heute einzig bekannte Ausnahme: Oracle). Bei diesen sollte (zumindest zur Bereinigung möglicher Verkettungsfehler einer Datenbank) gelegentlich ein application-consistent Backup erfolgen.

## 4.10 DP-Agents vs. agentless (Application-Support ohne Backup-Client Installation)

Bei **agentenbasierten Sicherungen** werden spezielle auf die zu sichernden Daten abgestimmte Software Komponenten installiert, welche z. B. mit einem Datenbanksystem kommunizieren und über dessen Schnittstelle Daten sichern oder wiederherstellen.

Bei einem **agentenlosen Backup und Recovery** wird kein auf die Applikation ausgerichteter Code vorinstalliert. Es gibt folgende Ausprägungen:

- Durch Installation eines neutralen Klienten, der sich den ausführbaren Code zum Zeitpunkt des Backups oder des Restores nach Bedarf lädt.
- Oder durch Nutzung von OS-nahen Grundfunktionalitäten (wie Microsoft VSS), welche (bei gesetzter Berechtigung) das Hineinschleusen von ausführbarem Code in die Applikationsserver ermöglicht.
- Eine Reihe von agentenlosen Lösungen verlässt sich nur auf die Nutzung von OS-nahen Grundfunktionalitäten (wie Microsoft VSS) und bietet keinen ausführbaren Code für die Restore-Prozesse.

Agentenbasierte und agentenlose Lösungen haben letztendlich die Applikation zu kennen und über deren APIs eine tiefe Integration zu gewährleisten. Dies ermöglicht es schon während einer Sicherung logische Inkonsistenzen in den zu sichernden Daten zu erkennen und entsprechen zu handhaben.

Der Vorteil von agentenlosen Backups bzw. Recoveries liegt im vereinfachten Rollout von Backup-Software, der vereinfachten Wartung (Softwareverteilung erübrigt sich) und oft auch in verringerten Fehlerquellen durch dynamisch richtige Handhabung von Änderungen beim zu sichernden Server (z. B. beim Versionsstand, Betriebssystemkomponenten, Patchleveln, Zusatzinstallationen uvm.).

Fehlen beim agentenlosen Ansatz genügend beherrsch- und reproduzierbare Restore-Funktionalitäten, sollte man den agentenbasierten Ansatz erwägen.

Sofern nicht alles befriedigend genug agentenlos gesichert werden kann, wird man in der Praxis häufig eine Kombination von agentenlosen- und agentenbasierten Sicherungen einsetzen.

## 4.11 Hypervisor-Level vs. VM-internal Backup

Auf die Grundproblematiken für DP&R von virtualisierten Servern wurde bereits im Kapitel 2.5 eingegangen.

VM-interne Backups haben den Nachteil, dass jeder IO von virtuellen auf physische Adressen übersetzt werden muss (mehr Overhead entsteht).

Hypervisor-Level Backups haben diesen Nachteil zwar nicht, aber Sie machen logische Restore-Prozesse auf Applikationsobjektebene der VM teilweise schwierig, oder gar unmöglich.

Hypervisor-Level Backups haben den Vorteil, dass die gesamte virtuelle Maschine inklusiver Konfigurationsdaten zur VM (Netzwerk, Partitionierung, Ressourcen, etc.) mitgesichert werden. Damit ist ein Disaster Recovery einfach möglich.

Die Software-basierten Snapshots der Hypervisoren dienen oft als Hilfsmittel, aus denen die Backup-Prozesse Ihre Sicherungsstände bekommen. Diese Snapshots haben aber typischerweise aufgrund der meist verwendeten ROW-Logik (siehe Kapitel 5.4) einen negativen Einfluss auf die Gesamtperformance. Vor allem beim Auflösen der Hypervisor-Snapshots können hier erhebliche Problem entstehen (besonders wenn die VM während des Backups schreibintensiv ist und/oder die Hardware gut ausgelastet ist).

Array-Snapshots der Disksubsysteme können hier wesentliche Vorteile bieten. Die Hauptproblematik ist hier meist, dass ganze Datastores = Volumes gleichzeitig in einen Applikations-konsistenten Zustand gebracht werden sollen, was bei hoher Anzahl von VMs sehr viele Minuten dauern kann.

Überhaupt ist das Herstellen der Applikationskonsistenz meist nur für einige der Applikationen möglich, so lange die DP-Software nur die Standard-Schnittstellen des Hypervisors und der oft mitgelieferten Integration von Microsoft für VSS-affine Applikationen bietet.

Aus den letztgenannten Gründen versuchen DP&R Tools zunehmend, für crash-konsistente Backupstände aus Hypervisor-Ebene mehr Restore-Funktionen zu bieten. Siehe auch Crash- vs. Application-Consistency (Kapitel 4.9). Sofern dies gegeben ist, ist oft ein Mix aus häufigeren crash-consistent Backups mit gelegentlichen application-consistent Backups überlegenswert.

Letztendlich ist es für die Praxis oft sinnvoll, einen Mix von DP&R Methoden einsetzen:

Alles, was sich nach Hypervisor-Level Backups nicht vernünftig logisch wiederherstellen lässt, wird man in der VM mit Methoden sichern, welche auch auf physischen Servern anwendbar sind.

Alles, was sich nach Hypervisor-Level Backups vernünftig logisch wiederherstellen lässt, wird man nur noch auf Hypervisor-Ebene sichern. Vor allem alle VM-Definitionen und die Boot-Disks der Guest-OS sind hier gute Kandidaten (lösen die letzteren doch das Windows »Bare-Metal Recovery« Problem sehr effektiv).

## 4.12 Starten von Diensten bzw. Anwendungen direkt aus dem Backup

Inzwischen sind erste Datensicherungslösungen in der Lage, wiederherzustellende Disks (ggf. ganze Server) direkt vom disk-basierten Backup-Medium in Betrieb zu nehmen.

Dies hat den Vorteil, dass wiederherzustellende Server wesentlich schneller wieder betriebsbereit sind und dass im Falle eines Ausfalls des Primärspeichers sofort eine betriebsbereite Umgebung zur Verfügung steht. Die Wiederherstellungszeit für hochkritische Server wird dadurch fast auf die reine Boot-Zeit reduziert.

Allerdings wird dies häufig aufgrund der limitierten Leistungsfähigkeit der Backup-Medien für den Produktiveinsatz nur sehr eingeschränkte Services erlauben.

Hinzu kommt hier auch oft ein Overhead für die Zwischenlogik des Backupsoftware-Herstellers und für eine erhöhte Fragmentierung auf den Backupmedien. Storage-Snapshots können hier ähnliches meist wesentlich leistungsfähiger anbieten.

Außerdem stellt sich die Frage, wie einfach ein Failback vom »Notbetrieb« auf die (ggf. neu zu beschaffende) Primärhardware zu handhaben ist und ob weitere Backups und Restores während des »Notbetriebs« möglich sind.

Teilweise wird die Funktionalität für physische Server geboten. Einige davon bieten Tools, die eine Transformation hin zu virtuellen Diskformaten oder weg von virtuellen Diskformaten erlauben. Auch Datenbanken bieten teilweise diese Funktionalitäten.

Noch häufiger werden derartige Lösungen für Virtualisierungsumgebungen mit Hypervisor-Level-Backup geboten. Nach dem Start ist die VM zu 100% verfügbar und operativ.

Bei all diesen Lösungen ist neben dem beschleunigten Restore-Prozess eine Anwendung für Test- und Entwicklungszwecke verbreitet.

Alle diese Lösungen zerstören typischerweise nicht die Backups, sondern Speichern die neuen Differenzblöcke (z. B. über eine Snapshot-Technik) separat.

## 4.13 Trend zu Image-Level Backups

Früher waren ausschließlich **File-Level Backups** üblich, welche folgende **Vorteile** haben:

- Ein logischer Medienbruch ist sehr einfach realisierbar.
- Es können nur Teile eines Daten-Volumes, z. B. bestimmte Verzeichnisse, gesichert werden.
- Eine Suche nach Versionsständen über Filenamen und andere File-Attribute ist über den DP-Katalog (der hier fast immer mit erzeugt wird) über alle Daten-Volumes hinweg relativ einfach möglich.

**Image-Level-Backups** verbreiten sich nun zunehmend, denn diese haben andere **Vorteile**:

- Eine hohe Anzahl enthaltener Dateien (> 10 Millionen pro Volume wird üblich) in Verbindung mit kleinen Dateigrößen vermindern hier die Backup-Geschwindigkeit nicht (wohingegen die File-Level-Backups sehr viele Random-IOs benötigen, da sie die Dateien sortiert nach Verzeichnis- und Dateinamen sichern).
- Da Image-Backups sehr wenig Logik benötigen, sind diese oft robuster und zuverlässiger. Z. B. besteht keine Gefahr, dass Änderungen unerkannt bleiben (was u. A. bei Rechteänderungen über eine File-Level-Logik schwieriger zu erkennen ist).
- Falls man auf eine »Heuhaufen-Suche« verzichten kann (siehe unten) – der DP-Katalog wird nicht durch sehr viele Einträge pro Datei-Version aufgebläht (und als Folge dessen dann eventuell selbst zum Backup- und Restore-Problem).
- Deduplication / Compression-Vorteile der Datenspeicherung bleiben erhalten.

Image-Level-Backups werden für folgende Anwendungsfälle gewählt:

- Sicherung von unstrukturierten Daten mit sehr vielen Millionen (oft kleiner) Dateien, die man anders nicht mehr in der geforderten Zeit gesichert oder wiederhergestellt bekommt.
- Virtuelle Disks von virtualisierten Servern/Klienten

Technische Hinweise zu Image-Level-Backups/Restores:

- Auch LUNs (Block-Storage Volumes) können als Image gesichert werden.
- Differentielle Snapshots (4th Gen DP) sind die effizienteste Art, Images zu sichern.
- Ein Restore auf Volume-Level ist immer einfach und effizient möglich (was z. B. die Disaster-Recovery beschleunigt).

- Ein Restore auf logischer File-Ebene aus dem Image-Backup ist oft auch möglich: z. B. über das Clonen und Mounten des Images und Herauskopieren der benötigten logischen Teilelemente, was durch eine DP-Software automatisiert werden könnte.

- Dort, wo eine »Heuhaufen-Suche« nach Filenamen und -versionen gefordert ist, ist nach dem Image-Erzeugen ein Aufbau des File-Indexes in einem DP-Katalog notwendig. Dies wird teilweise über schnelle proprietäre Differential-Schnittstellen von Storage-Herstellern unterstützt.

## 4.14 Backup2Cloud - Fähigkeiten

Vorteile von »Cloud Speichern« als Backup-Ziele (BaaS / DPaaS / DRaaS Dienste, die als Backup-Ziel Public oder Private Cloud-Targets benützen):

- sehr preisgünstige Diskkapazitäten
- sehr kurze Bereitstellungszeiten
- verbrauchsabhängige Abrechnung (ohne große Investitionen)
- räumliche Trennung von den Kundenrechenzentren
- breitbandig und mehrfach ausgelegte, günstige Internetzugänge

Typische Vertreter für Public Cloud Storage sind hier Amazon AWS S3 oder Microsoft Azure.

Ein elementares Grundprinzip bei der Gestaltung von Backup-Konzepten ist die räumliche Trennung der Backup-Daten von den Produktionsdaten. Bis dato wurde dies meist durch den Einsatz von physischen Tapes oder die optimierte Replikation von Backup-Daten auf einen zweiten Standort realisiert. Backup2Cloud (B2C bzw. B2D2C) bietet hierfür eine Alternative und dürfte vor allem Backup2Tape (B2T) bzw. Backup2Disk2Tape (B2D2T) teilweise ersetzen.

Mehrere unterschiedliche technische Ansätze sind möglich:

- Einsatz eines Backup Servers in der Cloud, d. h. der Backup Client sichert und überträgt seine Backupdaten über das Internet zu einem cloudbasierten Backup Server. Hierbei werden sehr häufig Datenreduktionstechniken wie Komprimierung und Deduplication (Client und Server) eingesetzt um die verfügbare Internetbandbreite so gering wie möglich zu belasten.

- Einsatz eines »Cloud Gateways«. Dieses Gateway kann von der Backup-Software oder über virtuelle oder physische Appliances bereitgestellt werden. In diesem Fall bauen ein oder mehrere Gateways eine Verbindung zum Cloud-Speicher auf. Somit ist das Cloud-Gateway (mit seinem Cloud-Speicher) ein zusätzlicher Backup-Medienpool, welcher typischerweise wie Disk oder Tape angesprochen wird. Siehe dazu auch das spätere Kapitel »PBBA Backup Cloud Gateway Appliances«

Es ist für Kunden von Vorteil, wenn die verbreiteten Cloud-Protokolle unterstützt werden (denn dies erlaubt mehr Auswahl bei den Anbietern).

Elementar wichtig erscheint beim Backup2Cloud, dass **eine starke und möglichst frühzeitige Verschlüsselung** stattfindet (idealerweise sollten dem Cloud-Provider die Daten zu keinem Zeitpunkt unverschlüsselt vorliegen).

- Falls die Verschlüsselung auf der Cloud-Seite aufgelöst wird oder werden muss, kann die Frage der Verschlüsselungszertifikate wichtig sein.

- Für den Zugriff im Recovery Fall ist ein zuverlässiges Schlüssel-Management wichtig.

Die datenschutzrechtlichen Aspekte werden in der Anlage behandelt.

Die Verfügbarkeitsgarantien der Cloud-Provider sollten bedacht werden und die eingesetzten Lösungen sollten vorübergehende Störungen einfach überbrücken können.

### Cloud2Cloud Backup

In der Public Cloud werden immer mehr Applikationen angeboten (Application as a Service – AaaS Dienste). Typischerweise sollten diese Angebote die Backup- und Recovery-Funktionen beinhalten. Techniken wie für Backup2Cloud scheinen dann dafür auch besonders geeignet.

Bei Private-Cloud-Betrieb im eigenen Unternehmen stellt sich die Frage wie Server bzw. Anwendungen, die in einer Cloud-Infrastruktur betrieben werden, in das Unternehmens-Backup-Konzept integriert werden können. Falls hier die Integration mit den eigenen Backup-Software-Komponenten nicht einfach möglich ist, bieten sich auch hier die obigen Backup2Cloud Lösungen an.

## 4.15 Endgeräte Backup/Wiederherstellung

Backup-Konzepte sollten neben den im Rechenzentrum befindlichen Daten auch Lösungen für die Sicherung der Daten der Endbenutzergeräte umfassen.

Die Problematik der Endgerätesicherungen hat sich in den letzten Jahren massiv verändert und verschärft, da der Trend immer mehr zu mobilen Geräten geht, welche sich zumindest teilweise außerhalb der Firmennetzwerke bewegen und deren Design wenig Verwandtschaft mit den im Rechenzentrum verwendeten Techniken aufweist.

Die **traditionellen PCs und Workstations im Firmennetzwerk** können weiterhin mit klassischen Methoden gesichert werden. Die hier übliche Methodik ist weitgehend mit dem klassischen agentenbasierten Server-Backup zu vergleichen. Fast alle klassischen Unternehmens-Backup-Lösungen bieten Agenten für Desktop-Betriebssysteme an.

Noch effizienter können **virtualisierte Desktops** gesichert und wiederhergestellt werden. Hier ist eine enge Verwandtschaft der Methoden für das Backup virtualisierter Server gegeben. Eine Reihe der auf das Backup virtualisierter Server spezialisierter Backup-Lösungen ist auch für Desktop-Virtualisierung geeignet.

Viel schwieriger und vielfältiger wird die Aufgabenstellung beim **Backup von mobilen Endgeräten wie Laptops, Tablets und Smartphones**:

Sofern sich diese Geräte nur selten oder nie im Firmennetzwerk aufhalten, benötigt man für die Sicherung Methoden, die mit relativ wenig Datenbewegung auskommen (3rd Generation DP wie Clientside-Deduplication oder Granular-Incremental-Forever) und über verschlüsselte Internetverbindungen in einen Backup-Standort sichern.

Für alle mobilen Geräte gilt, dass sich hier zunehmend die private und dienstliche Nutzung überschneidet, was auch datenschutzrechtliche Konsequenzen haben kann; z. B. wer darf Einblick in die privaten und dienstlichen Daten / Mails der Benutzer bekommen?

Sofern hierbei der gesetzliche (siehe Anlage) oder innerbetrieblich notwendige Datenschutz beim Backup-Standort (auch ein externer Cloud-Provider/Dienstleister) nicht genügend gewährleistet werden kann, sollte die Verschlüsselung schon vor dem Senden erfolgen und später nicht aufgebrochen werden, um datenschutzrechtliche Risiken zu minimieren.

Bei Tablets und Smartphones und anderen Geräten aus dem Consumer-Umfeld kommt hinzu, dass hier meist Betriebssysteme im Einsatz sind, welche wenig Gemeinsamkeit mit den im Rechenzentrum durch die IT betriebenen Systeme hat. Außerdem sind diese Geräte zunehmend nicht mehr im Eigentum den Unternehmens (BYOD=»Bring your own device«), was die Vielfalt der Geräte, Softwarestände und installierte Applikationen noch deutlich erhöht.

Daher ist es hier meist üblich, die auf das jeweilige Betriebssystem spezialisierten (oft im Standard mitgelieferten) Backup-Werkzeuge zur Sicherung einzusetzen. Diese bieten meist keine oder nur sehr beschränkte Möglichkeiten, diese mit den Backup-Methoden des Rechenzentrums zu integrieren.

Um die vielfältigen Problematiken in den Griff zu bekommen, können folgende Überlegungen (z. B. über ein Mobile Device Management) hilfreich sein:

- Vermeidung der Speicherung von nicht frei zugänglichen Firmendaten bzw. Mails auf den mobilen Endgeräten, indem man diese nur Online nach Authentifizierung zur Verfügung stellt:
  - z. B.: Durch Einsatz von Desktop-Virtualisierung
  - z. B.: Durch Einsatz von speziellen Apps, welche online auf Firmendaten zugreifen
- Backup dafür weiterhin nur in der Zentrale.

- Sofern dezentral firmensensitive Daten gespeichert werden müssen:
- Teilweise firmeneingerichtete Endgeräte zur Verfügung stellen, deren private Nutzung (mindestens formal) eingeschränkt ist und deren Datenaustausch mit Public-Cloud-Anbietern verhindert oder verboten wird.
  - Die dezentralen Datenträger sollten hier immer verschlüsselt gespeichert werden
  - z. B.: Automatisierte Replikation von Änderungen zur und von der Zentrale (bei Netzzugang)
  - z. B.: Zur Verfügung stellen von firmeneigenen Unternehmens- »DropBoxes« für die Datenablage
- Den Rest an Daten, Programmen und OS (meist nur für Linux/Windows basierte Geräte) über hoch verschlüsselte Backups (3rd Generation) sichern, zunehmend Richtung Public-Cloud-Provider (auch um Datenschutzprobleme für Privatdaten und Kostenprobleme zu minimieren).
- Meist sollte man sichere Login-Passworte, einen aktiven Virenschutz, lokale Verschlüsselung auf den Medien und evtl. auch eine automatische Datenzerstörung nach vielen erfolglosen Login-Versuchen erwägen.

Da der Hauptfokus dieses Leitfadens bei B&R liegt, können Security-Aspekte nur grob angedeutet, aber nicht vertieft behandelt werden.

## 4.16 Energieeffizienzunterschiede der Backup-Methoden und -Medien

Der Energieverbrauch ist sicher in den meisten Fällen nicht das primäre Entscheidungskriterium für eine Datensicherungslösung, sondern die Zuverlässigkeit, die Geschwindigkeit der Backup- und Wiederherstellungsprozesse als auch die Gesamtkosten dafür.

Die Energieeffizienz der Backup-Lösung wird man oft als einen Teil der Gesamtkosten bewerten. Hier ist zu bedenken, dass Datensicherungslösungen zyklisch Backup-Daten bewegen und mehrfach speichern müssen. Die dafür notwenige Infrastruktur verbraucht Energie. Restore-Prozesse fallen energetisch gesehen aufgrund der seltenen Notwendigkeit kaum ins Gewicht.

Einige Faktoren, die Auswirkungen auf die Energieeffizienz der Backup-Prozesse haben:

- Die Anzahl und energetische Leistungsklasse der für den Backup-Prozess eingesetzten Infrastrukturkomponenten (z. B. Server, Netzwerk-Komponenten, Anzahl drehender Disks und zugreifender Bandlaufwerke)
- Die Zeitdauer der Inanspruchnahme (welche vor allem durch die bewegte Datenmenge beeinflusst wird; z. B. granulare Incremental- gegenüber Full-Backups)
- Die benötigte Speicherkapazität aufgrund der Anzahl der Sicherungsstände und Aufbewahrungsfristen (ein Hinterfragen dieser kann sinnvoll sein) und der eingesetzten Verdichtungsverfahren (wie Deduplication)
- Die Art der eingesetzten Backup-Medien (Offline Medien wie Bänder haben die beste Energiebilanz).

Da die Backup-Methodik (1st bis 4th Generation) mehrere der oben genannten Faktoren wesentlichen beeinflusst, hat diese in der Regel die größte Auswirkung auf die Energieeffizienz.

Bezüglich des typischen Stromverbrauches einzelner RZ/IT-Komponenten empfiehlt sich das Studium des Bitkom-Leitfadens ↗Energieeffizienz in Rechenzentren.

## 4.17 Software Defined Data Protection (SDDP)

Software Defined Data Protection (SDDP) beschreibt einen Trend, bei dem immer mehr Backup-Funktionalitäten in die Backup-Software integriert oder Backup-Systeme (z. B. PBBAs) in Form von virtuellen Maschinen angeboten werden. Durch die heute auf Universal-Server-Hardware zur Verfügung stehende höhere parallele Rechenleistung können diese Funktionalitäten immer öfter über Software zur Verfügung gestellt werden. Funktionalitäten wie zum Beispiel Backup-Daten Replikation oder Deduplizierung benötigten in der Vergangenheit dafür oft spezialisierte Hardware. SDDP vereinfacht die Bereitstellung, das Erneuern und die Nutzungsoptimierung der Hardware, wodurch auch die Cloud-Fähigkeit einfacher zu erreichen ist.

## 4.18 NDMP

Das Network Data Management Protocol (NDMP) ist eine standardisierte Schnittstelle, über die es möglich ist, Backup- und Restore-Operationen unter direkter Beteiligung von Storage Systemen mit einer Backup-Software zu steuern. Typischerweise wird dies für Fileservices von NAS-Storage-Systemen benützt.

Die NDMP Client-Server Architektur separiert den Kontroll- und den Datenfluss durch die Aufgabenteilung und Kommunikation zwischen dem NDMP Client (DMA) und den NDMP Serverprozessen (Services):

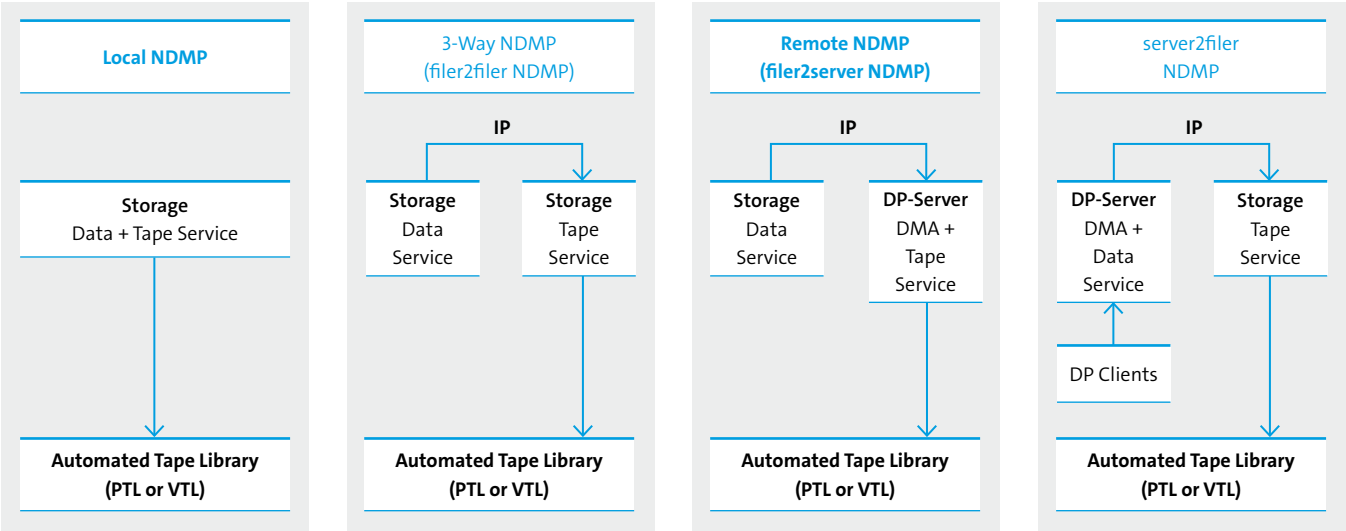
- Die **DMA** (=Data Management Application): ist die steuernde Instanz und wurde in vielen Backup-Software Produkten implementiert. Sie initiiert, kontrolliert und überwacht eine NDMP Session.

- Der **Data-Service** hat die Daten beim Backup in NDMP-Blöcke umzuformen bzw. beim Restore die NDMP-Blockinhalte ins Filesystem zu speichern.

- Der **Tape-Service** hat die NDMP-Blöcke beim Backup auf das Backup-Medium (ursprünglich war nur Tape möglich) zu speichern und beim Restore davon zu lesen. Beim Datentransfer kommuniziert dieser mit dem Data-Service.

- Der **NDMP SCSI-Pass-Through-Service** wird typischerweise zum Steuern des Media-Changers beim Wechseln von Bandkasetten in einer Tape Library genutzt. Er ermöglicht es der Backup-Software (DMA) SCSI-Befehle an ein SCSI Gerät zu senden, welches am NDMP Tape-Service angeschlossen ist.

Nachfolgend eine Übersicht der verschiedenen NDMP Modi (»NDMP Local Backup« und »NDMP Remote Backup« werden am häufigsten verwendet):




Source: NetApp

Abbildung 17: NDMP Modes

- Jeder NDMP-fähige Storage muss den Data-Service und den Tape-Service bieten.

- Alle DMA können »Local NDMP« steuern, viele auch »3-Way NDMP«.

- Sofern die Backup-Software auch Logik für einen eigenen Tape-Service bietet, ist »**Remote-NDMP**« anwendbar: Dies verbreitet sich seit der Verwendung von 10 Gbit Ethernet zunehmend, da damit keine Storage-Zertifizierung mehr für Tape-Drives und -Roboter notwendig ist. Außerdem bieten damit einige DMAs Tape-Multiplexing für NDMP-Datenströme und/oder NDMP Backups auf Disk-/Cloud-Backupmedien.

- Sofern die Backup-Software auch Logik für einen alternativen Disk-Service bietet (was eher selten ist), ist »**server2filer NDMP**« anwendbar: Dann können normale Backups der DP-Software in NDMP-Blöcke umgeformt und über eine am Storage-System angeschlossene Tape-Library gesichert werden.

Seit der NDMP Version 4 sind NDMP Features über sogenannte Extensions erweiterbar. Diese werden dann nicht von allen DMAs und auch nicht von jedem Storage unterstützt.

Einige wichtige Beispiele dazu:

- Image-Backups (per »SMTape« von einem der Storage-Hersteller) werden immer häufiger verwendet, da dies für NAS-Volumes mit sehr vielen Millionen File-Einträgen keinen von der Dateianzahl abhängigen Aufwand betreiben muss. Da ergänzend alle Snapshots beinhaltet sind und die Vorverdichtungen des Storages für das gesicherte Volume erhalten bleiben, wird damit nicht nur ein sehr schnelles Backup sondern auch die schnelle Wiederherstellung kompletter Volumes nach einem Disaster ermöglicht.

- »Restartable Backup«: Abgebrochene Sicherungen können wieder aufgesetzt werden, ohne dass die Restore-Fähigkeit leidet.

Für NDMP-Backups ist eine Storage-Hersteller-Abhängigkeit gegeben (siehe dazu Kapitel 6.1.2.2).

Mehr zum Grundsätzlichen siehe Fachbegriffserklärung »NDMP«.

# 5 DP&R-Hardware, -Medien und deren Trends

# 5 DP&R-Hardware, -Medien und deren Trends

## 5.1 Tape als Backup-Medium

Tape-Medien sind eines der ältesten Medientypen, die man in der Datensicherung verwendet. Obwohl es früher unvorstellbar war eine Datensicherung ohne Tape zu realisieren ist in der heutigen Zeit ein Trend zu einer »Tapeless« Datensicherung erkennbar. Dennoch hat das Medium Tape Vorteile gegenüber modernen Diskspeichertechnologien, die vor allem im Preis pro Terabyte liegen. Auch sieht man mehr so genannte »Flape« (=Flash-beschleunigtes Tape) Ansätze in der Datensicherung, bei welchen die Vorteile eines Flashspeichermediums (sehr schnelle Lese- und Schreibfähigkeit) mit den Vorteilen des Tape-Mediums (Speicherung großer Datenmengen) kombiniert werden.

### Vorteile von Tape-Medien:

- Tape-Medien bieten auf absehbare Zeit den günstigsten Preis pro TB aufgrund ihrer sehr hohen Kapazität
- Es entsteht kein Stromverbrauch, sobald das Tape-Medium entladen ist
- Tape-Medien bieten eine sehr hohe Lese- und Schreibrate bei sequentieller Nutzung
- Es entsteht keine nennenswerte Wärmeentwicklung durch die Nutzung von Tape-Medien
- Tape-Medien können ausgelagert werden. Dies ist unter anderem wichtig, falls die Datensicherung in einen separaten Brandabschnitt transportiert werden muss oder eine zweite Kopie an einem entfernten Standort aufbewahrt werden soll und andere Übertragungstechniken aufgrund einer zu großen Datenänderungsmenge scheitern
- Tape-Medien sind gegen einige äußere Einflüsse (wie ätzende Dämpfe, Überspannung, Feuchtigkeit) widerstandsfähiger als andere Datensicherungsmedien
- Es besteht ein hoher Schutz vor Schadsoftware und/oder Hackern

### Bevorzugte Einsatzgebiete für Tape bei Backup/Restore:

- Tape ist meist das sinnvollste Medium für Backupstände, die älter als Monate sind und es wird oft für sogenannte Langzeitbackups oder Compliance-Anforderungen genutzt
- Backup bzw. Restore von ganz großen Einzelobjekten (Datenbanken, Filme usw.) durch die hohe Lese- und Schreibrate bei sequentieller Nutzung
- Als zusätzliche Disaster-Kopie von Diskbasierten Sicherungen

## 5.2 Disk als Backup-Medium (kann Flash-beschleunigt sein)

Seit Jahrzehnten hat sich der Nutzungsanteil von Disk (im Vergleich zu Tape) als Backupmedium immer weiter erhöht. Dieser Trend basiert auf folgenden **Vorteilen von Disk als Backup-Medium**:

- Disks haben einen relativ geringen Laufwerkspreis
- Disks positionieren in Millisekunden auf jede Speicherstelle
- Disks erlauben durch die Random-IO-Fähigkeit parallele Backup- und Restore-Prozesse
- Disks kann man einfach im RAID-Verbund betreiben, was einen unterbrechungsfreien Betrieb bei Ausfall von Laufwerken ermöglicht
- Disk passt zu inkrementellen Backup-Methoden (da die Restores wesentlich schneller durchführbar sind als bei Tape).
- Disk passt zu incremental-forever Backup-Methoden, welche über relativ schmale WAN-Bandbreiten eine sehr frühzeitige Auslagerung von Backups in sicher getrennte Brandabschnitte ermöglicht (was den zeitlichen Datenverlust bei Disastern verringert).
- Disk eignet sich für DP-Deduplication (siehe 5.3)
- Disk eignet sich aufgrund der Direktzugriffseigenschaften für Snapshot-Techniken

Flash beschleunigte Disks, in Zukunft evtl. auch Flash-Only Medien, können die oben genannten Vorteile weiter verbessern, sofern der derzeitige Mehrpreis dies rechtfertigt.

## 5.3 Datenverdichtung für Backup-Medien (Deduplizierung, Komprimierung)

Da auf Backup-Medien viele Sicherungsstände produktiver Daten zu halten sind, sprechen folgende **Hauptgründe für den Einsatz von Verdichtungsmethoden**:

- Die Verringerung des Medienbedarfs spart Medienkosten und teilweise auch Energiekosten bzw. erlaubt es mehr Sicherungsstände wirtschaftlich zu halten.
- Die Verringerung der zu übertragenden Datenmenge ist teilweise ergänzend von großer Bedeutung. Insbesondere, wenn dadurch die zeitnahe Übertragung der Backups in andere Brandabschnitte über begrenzt skalierende WAN-Verbindungen vorgenommen werden kann.

Übliche Verdichtungsmethoden für Backup-Medien:

- Verlustfreie **Kompression** verdichtet Daten auf weniger Platzbedarf.
  - Die dafür verwendeten verschiedenen Verfahren (Algorithmen) sind bewährt. Je mehr Algorithmen bei der Komprimierung geprüft werden, desto mehr steigt die CPU-Belastung. IO-Technisch ergibt sich bei komprimierbaren Daten immer eine Entlastung.
  - Daten sind sehr unterschiedlich stark komprimierbar. Während klassische Datenbanken oft ca. 3:1 verdichtbar sind, wird bei Office-Formaten (Text-Dateien, Tabellenkalkulationen usw.) in der Summe meist nur ca. 1,5:1 erreicht. Vorkomprimierte Audio- und Videostreams lassen sich i.d.R. nicht weiter komprimieren.
- Auch **Incremental-Backup-Verfahren** führen vom Ergebnis her zu einer Verdichtung der Backups.
- **Single-Instancing (SIS)**: vermeidet die Mehrfachspeicherung inhaltsgleicher Objekte. Dies ist als Vorentwicklungsstufe von Deduplication für Backup Zwecke einzustufen. Für objektbasierte Speicherungen ist dies jedoch weiterhin üblich.
- **Deduplizierung** (gebräuchlicher in Englisch: Deduplication) vermeidet die Mehrfachspeicherung inhaltsgleicher Datenfragmente. Da Deduplication beim Thema Backup immer mehr Verbreitung erfährt, wird nachfolgend darauf tiefer eingegangen.

Deduplication beinhaltet meist ergänzend eine nachfolgende Kompression der Datenfragmente.

Eine deduplizierte Speicherung setzt ein Direktzugriffsmedium voraus (Disk, zukünftig zunehmend auch Flash).

Auch deduplizierte Backups haben die zuvor genannten Vorteile, aber auch folgende Nachteile:

- Geringere sequentielle Lesegeschwindigkeit (für Restores und Tape-Kopien)
- Höhere Risiken des Datenverlustes aufgrund der Komplexität der Datenspeicherung

Man unterscheidet die eingesetzten Deduplication-Verfahren nach einigen Kriterien:

- **Fixed block Deduplication (FBD)** erkennt Dubletten nur auf Blockebene, während **Variable Byte Range Deduplication (VBR)** Datendubletten auch an beliebiger Stelle in Datenblöcken beginnend und auch blockübergreifend erkennt (was für die nachträgliche Deduplizierung klassischer Backup-Datenströme mit wechselnder Block-Belegung sehr wichtig ist).

- **Inline-Deduplication** reduziert die Datenmenge, bevor diese gespeichert wird; **Postprocess-Deduplication** dagegen erst im Nachgang (mehr Zwischenspeicher-Kapazität und Zusatz-IOs werden benötigt).

- Je nach Zeitpunkt des Deduplizierens im Backup-Workflow können Effizienz-Vor- oder Nachteile entstehen; ein »**Rehydration**« (=Enddichten) sollte nicht oft notwendig sein.
  Es gibt verschiedene Zeitpunkte, bei denen die Deduplication einsetzt oder aufgelöst wird:

  - Deduplication schon am Primärstorage

  - Bei der Replikation vom Primär- zu einem Sekundärstorage
    (Dedupliziert oder zuvor Rehydration)

  - Erst am Sekundärstorage

  - Beim Backup-Prozess schon beim Backup-Client (**Client side Deduplication**)

  - ... oder ab dem Backup-Server

  - ... oder erst beim Empfang in einer Dedup-fähigen Appliance

- Nach der Wirkungsbreite der Dublettenerkennung (**Deduplication Scope**):

  - z. B. Wirkung nur lokal innerhalb eines Daten-Volumes,

  - ... oder global auf Target-System-Ebene
    (z. B. über alle Daten in einer PBBA / einem Storage-System)

  - ... oder global über einen Cluster-Verbund
    (z. B. zwischen mehreren verschalteten PBBAs / Storage-Systemen)

Mit oder ohne Inkaufnahme eines winzigen **Hash Collision Risikos** ( »hash-based« verlässt sich auf die Eindeutigkeit des berechneten Hashkeys plus Elementlänge, absolute Verlustfreiheit kann nur eine Verifikation der Dateninhalte bieten (was unter anderem auch beim Verfahren »Grow-by-Compare« der Fall ist) – siehe ↗Wikipedia. Auf den rechtlichen Aspekt eines verbleibenden Risikos wird in der Anlage kurz eingegangen.

## 5.4 Snapshot Differenzblock-Techniken (für Disk- / Flash-Speicher)

Snapshot Technologien sind eine wichtige Säule für heutige Backup- und Recovery-Konzepte. Ein wesentlicher Vorteil ist, dass beim Backup (der Snapshot-Erstellung) keine Daten kopiert werden müssen. Dies erlaubt extrem schnell abgeschlossene Primär-Backups und somit häufigere Backups. Des Weiteren wird das Erstellen konsistenter Backups erleichtert.

Ein temporärer Snapshot kann die Basis für Backups der Generation 1, 2 oder 3 sein (siehe Kapitel 3).

4th Generation DP&R Konzepte bestehen dagegen aus:

- Dem Halten von einigen bis sehr vielen Snapshots über Tage bis Wochen.
- Dem Verbringen der Änderungszustände in andere (sicher getrennte) Brandabschnitte. Dies erscheint notwendig, um die Restrisiken des Primärstorages abdecken zu können (z. B. dem Löschen von Volumes mit den Snapshots, Hardware/Software-Problemen im Storage, RZ-Disaster usw.):
  - Entweder durch eine auf Snapshots basierte Replikation (eine blocklevel Incremental-Forever-Replikationen ist dafür am leistungsfähigsten)
    - Teilweise kann hier die Verdichtung (Deduplizierung / Kompression) schon am Primär-Storage beginnen und bei der Replikation erhalten bleiben.
    - Einige Lösungen bieten die Möglichkeit, hierbei einen logischer Medienbruch (Auflösung aller Storage-Pointer vom Primärdatensystem) durchzuführen.
  - Alternativ oder ergänzend durch die gelegentliche (z. B. wöchentliche) Ergänzung um eine DP Generation 1/2/3 Techniken. Dies ist besonders dann sinnvoll, wenn eine Langfristhaltung von Backups gefordert ist. Falls derartige Backups vom Sekundär-Storage erfolgen, ist man bei dieser Sicherung nicht mehr auf ein Backup-Zeitfenster beschränkt, da der Primärstorage von der hohen Backup-IO-Last befreit ist.

Das Zurücksetzen kompletter Daten-Volumes ist meist über Pointer-Veränderungen im Storage-System möglich. Dies kann Restore-Zeiten großer Datenbestände in wenigen Sekunden ermöglichen.

Für einen Restore logischer Elemente (z. B. ein einzelnes Mail) aus einem Block-Storage (LUN) oder aus einer Virtual Disk sollte außerdem ein differentieller Clone (siehe Fachbegriff »Clone«) zum Storage-Snapshot möglich sein, da manche OS nur den Zugriff auf Disks mit Write-Zugriff erlauben.

Es gibt mehrere alternative Snapshot-Verfahren, welche sich evolutionär in folgender Reihenfolge entwickelt haben und unterschiedlich effizient sind:

- **Full Copy Snapshots:** Da hier für jede Kopie die volle Speicherkapazität benötigt wird, ist dies für 4th Gen. 4 DP&R nicht sinnvoll und wird auch als Basis für Gen. 1 bis 3 DP&R nur noch selten verwendet.

- **Differentielle Snapshots** sind dagegen speicherplatzeffizient und von der Seite her für DP&R als interessant einzustufen. Obwohl jeder Snapshot ein logisches Full-Backup ist, werden hier neben dem aktiven Filesystem nur die Differenzen zu den Snapshots gehalten. Aus Data-protection-Sicht wäre es wünschenswert, viele Snapshots über viele Tage bis hin zu Monaten vorhalten zu können, ohne dass das Performance-Verhalten spürbar negativ beeinflusst wird. Die technischen Implementierungsansätze unterscheiden sich aber besonders im Performanceverhalten erheblich:

  - **Redirect on Write (RoW):** ist mit sehr hohem Aufwand beim Auflösen von Snapshots verbunden; daher wird hier üblicherweise nur ein einziger Snapshot temporär für ein nachfolgendes Backup gehalten. Derartige Snapshots finden sich vor allem bei Virtualisierungs-Hypervisoren und in Betriebssystemen.

  - **Copy on (first) Write:** da hier nur beim Überschreiben aktiver Datenblöcke ein wesentlich höherer Aufwand entsteht, kann man damit meist für einige Stunden bis wenige Tage Backups in Form von Snapshots vorhalten. Aber diese Technik ist nicht effizient genug, um Snapshots länger aufzubewahren..

  - **Write Anywhere (WA)** stellt die performance-technisch unkritischste Implementierung dar. Dadurch können hunderte von Snapshots über Wochen und Monate vorgehalten werden. Die Beimischung von DP&R Gen 1/2/3 Methoden kann selten erfolgen und ist teilweise verzichtbar. Da diese Methode sehr hohe Anforderungen an die Implementierungsreife der Storage-Systeme bezüglich Stabilität und Optimierung auf Sequential Write und Read stellt, ist die Anzahl der Anbieter noch sehr begrenzt.

Näheres zu den Snapshot-Techniken kann man über den Fachbegriff »Snapshot« nachlesen.

## 5.5 Purpose Build Backup Appliances (PBBAs)

Allgemein bezeichnet man ein System, welches ab Werk vorkonfiguriert geliefert und vom Kunden meist binnen Minuten einsatzfähig gemacht werden kann, als Appliance. Im Backupumfeld werden diese Systeme auch als Purpose Build Backup Appliances (PBBAs) bezeichnet. Dabei wird die Komplexität des Gesamtsystems so weit wie möglich vor dem Anwender versteckt und die Konfiguration auf das notwendige Minimum reduziert.

Neben **physischen PBBAs** für durchsatzstarke Anforderungen mit dedizierter Leistung werden auch immer mehr **virtuelle PBBAs** und teilweise beides mit der gleichen Funktionalität angeboten. Virtuelle Appliances setzen bestimmte Virtualisierungs-Infrastrukturen voraus, vermindern Hardware-Abhängigkeiten und vereinfachen die Automatisierung, was für Cloud-Umgebungen besonders wichtig ist.

Die Funktionen der PBBAs können oft auch durch eine Backup Software mit passender Hardware erzielt werden, aber PBBAs bieten als vorkonfigurierte »Black Boxen« mit minimaler Infrastruktur folgende Hauptvorteile gegenüber traditionellen »do it yourself« Lösungen:

- **Konsolidierungseinsparungen**: Durch die meist höhere Skalierung ist oft eine deutliche Senkung der Anzahl von DP&R Geräten möglich.
- **Einfacherer Wartungsaufwand und Support Modell**: Patches und Updates für alle Systemkomponenten werden bereitgestellt und »single point of contact« bei Support Problemen ist gegeben.
- **Bewährte, getestete und optimierte Konfiguration**
- **Klar definierte Leistungsfähigkeit**

All dies resultiert in der Regel in:

- **Vereinfachung und Beschleunigung der Anschaffung und Inbetriebnahme**: PBBAs bieten Hardware (bzw. Virtualisierungsvorgaben), Software und Support in einer »schlüsselfertigen Lösung« von einem Hersteller. Somit erübrigt sich für IT- und Backup-Verantwortliche der Kosten- und Zeitaufwand für Recherche, Auswahl, Kauf und Bereitstellung einzelner Ressourcen und Teile, welche dann noch mühselig zusammengefügt und getestet werden müssten.
- **Reduzierung der Betriebskosten**: PBBAs sind in sich optimiert, daher bestens geeignet um den Platzbedarf, Strom- und Kühlungskosten im Rechenzentrum zu reduzieren. Durch den Appliance-Ansatz und mehr Homogenität sinkt auch der Administrationsaufwand für den Betrieb.

Deduplizierung und WAN-optimierte Replikation sind Bestandteil der meisten PBBAs.

Der PBBA Markt beinhaltet unterschiedliche Typen von Appliances. Auf die wesentlichen wird in den nun folgenden Subkapiteln eingegangen.

### 5.5.1 Backup Target Appliances zur Disk-Optimierung

Diese PBBAs haben meist einen Schwerpunkt bei der Deduplizierung und Replikations-optimierung von Backup-Datenströmen. Target-Appliances bieten einen Speicherpool der zwischen einigen TB bis zu mehreren PB nutzbaren Volumen liegen kann und beherrschen Deduplizierung (siehe 5.3).

Sie werden meist in Verbindung mit einer oder mehreren dafür zertifizierten Third-Party Backup Software Lösung(en) eingesetzt. Die Schnittstellen zu der Backup Software sind NAS (NFS/CIFS), Virtual Tape Library (VTL über FC-SAN/iSCSI-SAN) oder Hersteller-spezifische APIs, womit üblicherweise auch Deduplizierung an der Quelle erfolgen kann. Dies erlaubt dann eine verteilte Deduplizierungs-Logik, welche weniger Datenverkehr und eine höhere Skalierbarkeit erlaubt.

Die Replikation kann nur zwischen Appliances des gleichen Herstellers erfolgen und wird entweder innerhalb der Appliances gesteuert oder von der Backup Software über eine entsprechende Schnittstelle. Teilweise wird hinter der PBBA das Befüllen physischer Tapes unterstützt.

### 5.5.2 Backup Target Appliances zur Tape-Optimierung

Derartige Target Appliances sind besonders für Kunden von Vorteil, die sehr viele Daten (meist zur längerfristigen Aufbewahrung) auf physische Tapes schreiben möchten.

Meist geht damit eine Tape-Virtualisierung einher, die den angeschlossenen Servern wesentlich mehr virtuelle Tape-Laufwerke zur Verfügung stellt als physikalisch im Backend implementiert sind. Dadurch sind aufwendige Dynamic Tapedrive-Sharing Mechanismen als auch ein Tape-Multiplexing verzichtbar. In den meisten Fällen werden die Backup-Daten von der Appliance als virtuelle Tapes auf Disk zwischengespeichert und nachgelagert optimiert auf physikalische Tapes geschrieben. Da physikalische Tapes nur seriellen Datenzugriff erlauben und Tape-Laufwerke hohe Datenströme ermöglichen, erfolgt die Tape-Ausgabe in der Regel von einem nicht dedupli-zierten Format. Die Nutzung der Tapedrive internen Datenkomprimierung ist üblich. Bei Verwendung großer Tape-Libraries im Backend der Target Appliance können so i.d.R. Datenvolumen von bis zu mehreren hundert Petabyte gespeichert und verwaltet werden.

Der Disk-Speicherpool innerhalb der Target Appliance kann zwischen einigen TB bis zu mehreren PB nutzbaren Volumen liegen und unterstützt i.d.R. Deduplizierung.

Als Zugriffsschnittstellen für die Backup Server stehen Virtual Tape Library (VTL), evtl. auch NAS (NFS/CIFS) und/oder Hersteller-spezifische APIs zur Verfügung, womit oft auch eine Deduplizierung beim Sendeprozess erfolgen kann. Die Replikation kann nur zwischen Target Appliances des gleichen Herstellers erfolgen und wird entweder über die Appliances oder von der Backup Software über eine zertifizierte Schnittstelle gesteuert. Einige Target Appliances bieten neben einer Tape Option auch eine Cloud Schnittstelle an.

Durch den Einsatz von Backup Target Appliances können Probleme mit Tape-Handling, Tape-Migrationen, Zugriffsverwaltung, Backup-Kopieerstellung und Engpässe bei der Anzahl physischer Tapedrives weitgehend eliminiert werden.

### 5.5.3 Backup Server Integrated Appliances

Die Backup-/Media-Server der Backup-Software-Hersteller werden hier in Form vorkonfigurierter Appliances ausgeliefert.

Diese können auch Deduplizierung mit eigener Logik beinhalten und bieten alle üblichen Zugriffsschnittstellen an.

### 5.5.4 Backup Cloud Gateway Appliances

Verschiedene Anbieter bieten Gateway Appliances an, welche oft mehrere oder alle der folgenden Einsatzoptionen bietet:

- »on-premise« Backups in einen Cloud-Protokoll-fähigen Speicher innerhalb der Kundenlokationen
- Nutzung von Cloud-Providern für die Speicherung der Backups
- Nutzung der Technik in der Cloud, falls sich die Primärdaten auch dort befinden

Cloud Backup Appliances haben in der Regel lokalen Disk-Storage für ein schnelles Zwischenspeichern der letzten Backups und für deren Restore-Anforderungen, während der Cloud-Storage dann zeitversetzt aktualisiert wird und bei Restore älterer Backup-Stände und bei DR angesprochen wird.

Teilweise kann der lokale Disk-Platzbedarf auf einen Bruchteil der Gesamtblöcke auf dem Cloud-Speichern reduziert werden. Hierbei sollten die Zeiten für Restore SLAs beim Sizing berücksichtigt werden.

Meist ist eine Optimierung Richtung geringer WAN-Übertragungsbandbreite integriert.

Teilweise werden alle Cloud-Speicherzugriffe nur hochverschlüsselt vorgenommen.

Die DR-Readiness klassischer Backups ist damit im Vergleich zu anderen Lösungen relativ kostengünstig und mit wenig Aufwand erreichbar.

### 5.5.5 Backup Appliances für spezielle Datenbanken

Backup Appliances für Datenbanken wurden mit dem Ziel entwickelt, speziell für eine bestimmte Datenbank optimierte Systemkomponenten mit integrierten Backup- und Recovery-Verfahren zu bieten. Die datenverlustfreie Wiederherstellbarkeit der Datenbankanwendung steht dabei meist im Vordergrund.

Um auch die letzten Datenbank-Transaktionen wiederherstellen zu können, sind z. B. Methoden wie Log-Shipping von Schattendatenbanken implementiert.

Zur Minimierung der Backup-Prozesslast werden oft nach einer initialen Vollsicherung nur noch inkrementelle Sicherungen erstellt, ergänzt um virtuelle Full-Backups, die die Appliance nach jeder erfolgten inkrementellen Sicherung selbst erstellt und katalogisiert.

Typischerweise ist die Administration und das Monitoring der Appliance in das übliche DBAs-Tool der DB integriert.

# 6 Tipps zur Überarbeitung von DP&R-Konzepten

# 6 Tipps zur Überarbeitung von DP&R-Konzepten

In vielen Unternehmen bleiben Datensicherungskonzepte und -Strategien oft über Jahre hinweg unverändert. Veränderungen der IT-Landschaft oder auch bei der Nutzung der IT können jedoch zusätzliche Anforderungen an die DP&R-Infrastruktur in Richtung Funktionalität, Kapazität und Performance nach sich ziehen. Falls die Unterstützung durch die bestehende DP&R-Infrastruktur nicht möglich ist, entwickeln sich oftmals additive Hardware- bzw. Software-Infrastrukturen, die quasi als Silo für die Datensicherung bestimmter Anwendungen bzw. Umgebungen dienen.

Das DP&R-Konzept beschreibt den angestrebten Soll-Zustand und ist die Basis für das Betriebskonzept als auch eines Disaster-Recovery-Plans.

Das DP&R-Betriebskonzept beschreibt Zuständigkeiten und Workflows, um das DP&R-Konzept in der Praxis für den Normalbetrieb umzusetzen.

Der Disaster-Recovery Plan beschreibt die Prozesse, die im Sonderfall eines Desasters (z. B. Untergang eines Rechenzentrums) bedacht und durchgeführt werden sollten/müssen.

Eine turnusmäßige und strukturierte Herangehensweise bei der Erstellung und Überarbeitung von DP&R-Konzepten als auch des daraus abgeleiteten DP&R Betriebskonzeptes und des DR Plans hilft optimale Entscheidungen zu treffen. Das Ziel ist, für absehbare Zukunft gewappnet zu sein und die Risiken von Datenverlusten und Nichtverfügbarkeiten im Rahmen der Geschäftsanforderungen, Sicherheitsrichtlinien und Budgetgrenzen des Kunden, in sinnvoller Art und Weise zu minimieren.

## 6.1 DP&R-Konzept

Die Datensicherung und Wiederherstellung (Data Protection und Recovery) als auch Disaster Recovery sind Vorsorgen gegen Daten- und Verfügbarkeitsverluste. Der Fokus eines DP&R-Konzeptes liegt in

- der Minimierung von Datenverlustrisiken (also dass Daten komplett verloren gehen könnten), dazu muss es u. A. möglich sein, Daten zeitlich zurückzusetzen
- der Minimierung von Datenaktualitätsverlusten, falls man zeitlich zurücksetzen muss (RPO)
- der Minimierung der Zeitdauer für die Daten- und Service-Wiederherstellung (RTO)
- der Minimierung der Zeitdauer für die Erstellung des Backups (Einhaltung definierter Backupzeitfenster)
- als auch der Minimierung des Betriebsaufwandes (manueller Eingriffe, Investitionen usw.), um diese Ziele zu erreichen
- Umsetzung gesetzlicher Vorgaben (z. B. Datenlöschung – siehe in der Anlage)

Ein DP&R-Konzept sollte folgende Punkte beschreiben:

- Eine Grobdefinition der Geschäftsrisiken, die es ggf. zu minimieren gilt
- Die Grobbeschreibung der firmenweiten Rechenzentrums-Infrastruktur (mit Backup-Rechenzentren und Disaster-Standorten)
- Die technische Notfallvorsorge pro Rechenzentrum
- Die einzusetzenden bzw. eingesetzten DP&R Software- und Hardware-Architekturen
- Abgeleitete DP&R-Klassen (jeweils mit definierten DP&R SLAs und erwarteten Grobkosten)
- Die Beschreibung typischer Backup-/Recovery-Prozesse im Allgemeinen

Der betriebene Aufwand und Detailierungsgrad sollte adäquat zur Firmengröße gehalten werden.

### 6.1.1 Assessment

Die Durchführung von regelmäßigen (z. B. jährlichen oder 2-jährlichen) Assessments mit allen am DP&R-Prozess mittelbar oder unmittelbar Beteiligten ist essentiell um eine konsolidierte Übersicht der aktuellen und eventuell auch zukünftigen Anforderungen zu erhalten.

Ziele der Assessments sind die Anforderungen/Rahmenbedingungen zu folgenden Themen zu klären:

- **Aktuelle und zukünftige Anforderungen aus Applikations- und Betriebssicht:** Geänderte oder neue Geschäftsanforderungen an das Unternehmen wirken sich in der Regel auch auf die IT aus. Geänderte Soll-Verfügbarkeiten, neue Applikationen, wachsendes Datenaufkommen, usw. sind die Folge. Je früher auch die DP&R-Aspekte mit bedacht werden, je besser passt die IT-Lösung zu den Geschäftsanforderungen. Außerdem kann die Zeitdauer bis zum Produktivbetrieb verkürzt werden (z. B. durch frühzeitige Ausbildung des Betriebes)

- **Ermitteln der Bedrohungen für die IT-Services:** Eine individuelle und aktualisierte Risikoanalyse der Bedrohungen für die IT-Services bzw. Datenbestände hilft, das DP&R-Konzept auf Wirksamkeit zu überprüfen. Dabei sind bestehende aber auch neue Bedrohungen und deren Wichtigkeit für die eigene IT regelmäßig zu bewerten. Neben den bekannteren Bedrohungsszenarien, wie Katastrophen, Systemausfällen, Fehlfunktionen, Fehlbedienung, sollten Hackerangriffe, Virenbefall, Angriffe/Sabotage von »Innen«, usw. nicht vergessen werden.

- **Unternehmensvorgaben:** Unternehmensrichtlinien können in vielfältiger Weise das DP&R--Architekturkonzept beeinflussen. Zum Beispiel: Datenmanipulationssicherheit, Berechtigung und Datenschutz für sensitive Daten, Gebäudetechnik, Standortplanung, erhöhte Standortrisiken.

- **Gesetzliche Vorgaben:** Gesetzliche Vorgaben vor allem bezüglich der Datenschutzvorgaben sind unbedingt zu berücksichtigen (siehe Anlage), aber auch besondere Richtlinien der jeweiligen Industrie oder Branche sind zu befolgen.

- **IT Roadmap/strategische Entwicklung der IT im Unternehmen:** Generell sollte jede Neuausrichtung/Änderung der IT-Infrastruktur auch in Richtung DP&R-Konzept frühzeitig verifiziert werden (z. B. durch Aufnahme einer Verifikation im ITIL Change-Management Prozess). Steht beispielsweise für die kommenden Jahre eine Nutzung von Cloud-Services auf der Unternehmen-IT-Roadmap, so kann es durchaus sinnvoll sein, Cloud-Backups (to the cloud und/oder in the Cloud) frühzeitig mit in die DP&R-Strategie zu übernehmen. Ein weiteres Beispiel ist eine Strategie Richtung Server-Virtualisierung, welche darauf optimierte geänderte DP&R-Prozesse sinnvoll machen können.

- **Mengengerüste bestimmen:** Realistische aktuelle und zukünftige Anforderungen an Kapazität und Performance sind hilfreich, um nachhaltige Infrastruktur-entscheidungen zu treffen. Zu beachten ist dabei, welche SLA-Anforderungen an die zu sichernden Datenbestände gestellt werden (z. B. Anzahl der Backup-Kopien).

- **Konsolidierung der Backup-Infrastruktur:** Gerade in einer stark segmentierten Infrastruktur, mit unterschiedlichen parallel eingesetzten Backup-Systemen, sollte im Assessment eine mögliche Konsolidierung erwogen werden. Neben der einfacheren Planung von Mengengerüsten ist die Konsolidierung nach wie vor eine der wirksamsten Kostensenkungsmaßnahmen in der IT. Sowohl zu klein als auch zu groß dimensionierte Einzelsysteme verursachen Mehrkosten und/oder unnötige Kapitalbindung.

- **Auswirkungen von Störungen und Desastern auf das Business abschätzen:**
  Die Nichtverfügbarkeit der IT-Services, totale Datenverluste bzw. unnötig umfangreiche Datenaktualitätsverluste haben sehr unterschiedliche Auswirkungen auf das Geschäft und damit das Unternehmen. Da diese für die betriebenen Services oder genutzten Datenbestände sehr unterschiedlich vom Schadenspotential als auch von den SLAs her sind (Ausfall von Sekunden bis Tagen), bedarf es Einzelbetrachtungen und regelmäßiger Reviews.

- Meist macht es Sinn, diese **Abschätzung der jährlichen Risiken per Tabellenkalkulation** vorzunehmen:

  - Damit lassen sich Veränderungen bei den Kostenfaktoren, den Risiken und bei IT-Veränderungen sehr leicht neu durchrechnen und bewerten. Das gilt auch für die Bewertung möglicher Gegenmaßnahmen.

  - Letztendlich wird man einige Kostenfaktoren des Unternehmens benötigen und diese gelegentlich aktualisieren müssen (z. B. »Was ist die Firma insgesamt wert«, »Was kostet ein IT-Mitarbeiter / Verwaltungsmitarbeiter / Produktionsmitarbeiter pro Stunde«, »Wie viele Mitarbeiter sind in den verschiedenen Unternehmensbereichen betroffen«).

- Dann wird man pro Störungs-/Schadens-Szenario eine Zeile anlegen:
  - mit Schlagworten zum Szenario
  - mit erwarteter Schadenshäufigkeit in Jahren (z. B. 0,02 für ca. wöchentlich auftretende Events oder 300 für Disaster-Szenarien, welche nur alle 300 Jahre erwartet werden)
  - Der Stundenaufwand, den die IT-Verwaltung/Produktion beim Auftritt zur Bereinigung zu leisten hat
  - Der zusätzlich erwartete Business-Verlust im Markt (z. B. Konkurrenz bekommt kurz-
  - und mittelfristig mehr Aufträge, bewertet in € pro Event)
  - Daraus wird der zu erwartende statistische Schaden pro Jahr errechnet
  - Diese Angaben können bei den später erwogenen Maßnahmen in kopierten Zeilen des Istzustandes leicht in einen erwarteten Sollzustand umgesetzt werden, dem die Investitionen gegenüber zu stellen sind. Daraus ergibt sich ein ROI (Return-On-Investment).

### 6.1.2 Investitionen zur Verbesserung erwägen

- Ziel: Minimierung von Risiko-/Kostenrelation. Das heißt, Investitionen in DP&R-Verbesserungen haben sich wirtschaftlich über verminderte Risiken zu rechnen.

- Dies ist ein iterativer Abwägungsprozess, bei welchem auch Kreativität gefordert ist. Außerdem ist ein gewisser Marktüberblick zu neuen DP&R Techniken und eine gute Beurteilung des Reifegrades derselben von Vorteil. Aus diesen Gründen sollte besonders für diese Phase des Konzeptüberarbeitens die Hinzuziehung externer, erfahrener DP&R Konzeptberater erwogen werden.

- Bewerten der zu erwartenden Risikominimierung/Kostensenkung versus notwendiger Investition: dazu ist es oft am Sinnvollsten, einen ROI-Faktor (=Return of Investment) in Jahren für jede der erwogenen Maßnahmen zu berechnen.

- Den Umsetzungsplan wird man i.d.R. nach den ROI-Faktoren priorisieren (also die Maßnahmen vorziehen, die sich am schnellsten bezahlt machen). Abhängigkeiten zwischen den Einzelmaßnahmen oder Engpässe bei den Ressourcen (wie Mitarbeiter, Restlaufzeiten von Hardware oder Software) können die Reihenfolge jedoch zusätzlich beeinflussen.

- DR-Methoden sollten einfach beherrschbar sein und gelegentlich getestet werden (ein DR-Handbuch – auch wenn es für kleine Firmen kurz ausfallen dürfte – macht Sinn; siehe 6.4).

Nachfolgend wird auf typische Erwägungen zur Verbesserung eingegangen:

### 6.1.3 DP-Software ersetzen oder ergänzen?

Die Erfahrung zeigt, dass das vollständige Ersetzen einer Backup-Software durch eine andere ein oft sehr unterschätzter aufwändiger Prozess ist.

Insbesondere bei großen Firmen nimmt der Aufwand meist überproportional zu, was zum einen durch die Vielzahl der betroffenen Mitarbeiter, zum anderen auch sehr stark durch komplexe, funktionsstarke, für Großunternehmen designte Universal-Backup-Software bedingt ist.

Besonders unterschätzt wird hier oft, dass der notwendige Skill-Aufbau (Ausbildung und Aufbau praktischer Erfahrung) viel Zeit, Kosten und vorübergehende Störungen verursacht.

Auch die mangelnden Migrationsmöglichkeiten bestehender Backups mit langer Aufbewahrungszeit stellt in der Praxis ein sehr großes Problem dar.

Daher empfiehlt sich folgende Reihenfolge von Fragestellungen:

- **Bietet die eingesetzte DP-Software neue Funktionalitäten, die getestet und benutzt werden sollten?**

- **Ist ein Ergänzen um eine partiell leistungsfähigere DP-Software** für bestimmte Applikationen oder Virtualisierungen **sinnvoller** (= »Combine the Strengths« Strategie) als der Komplett-austausch einer Backup Software?

- **Ist teilweise die lockere Kombination von mehreren Backup-Methoden für einen DP&R-Workflow** sinnvoll (z. B. Snapshots auf Array-Ebene und Replikation durch eine DP-Software #1, anschließendes Tape Backup durch eine DP-Software #2)?

- **Macht der Einsatz von Converged Solutions Sinn?** Seit einigen Jahren nimmt die Verbreitung sog. »Converged Solutions« (auch als Teil von »Building Blocks«, mit Hardware oder in Cloud-Umgebungen) zu. Im Unterschied zur klassischen Bereitstellung von Einzelkomponenten wird hier i.d.R. eine Lösung fertig vorkonfiguriert als Einheit bereitgestellt. Meist verfügen diese Building Blocks über Management-Software, die auch die B&R beinhalten kann oder durch einen Backup-Block ergänzt werden kann. Jedes Unternehmen muss hier entscheiden, ob diese in sich abgeschlossenen Backup-Systeme oder nur eine in die vorhandene allgemeine Backup Lösung integrierte Lösung bevorzugt wird, zumindest wenn die Integration in allgemeine Backup Systeme über klassische Agenten möglich ist. Der Vorteil der Converged Solutions liegt in der meist schnelleren Implementierung und leichteren Automatisierbarkeit. Die Zuständigkeit für Backup kann in dem Fall oft zum Applikations- oder Building Block Verantwortlichen verlagert werden.

- Einsatz von **ObjectStore-Techniken** (siehe Kapitel 3.6) erwägen?

Falls man **komplett auf eine andere Universal-Software wechseln** will (»Single Pane of Glass« Strategie), stehen folgende Überlegungen an:

- Welche DP-Software ist wirklich die optimalste? Das muss in der Regel aufgrund der Tragweite und des heutigen/absehbaren Bedarfs aufwändig ermittelt werden.
- Nach der Entscheidung für eine andere DP-Software sollte am besten ein langfristiges Stufenkonzept bevorzugt werden, das die Umsetzung nach Applikations-Stacks in sinnvollen Einzelschritten ermöglicht. Ein zu hoher Zeitdruck birgt meist Risiken.
- Die Migration von Katalogen und Backup-Medien kann untersucht werden – aber diese wird meistens nicht sinnvoll durchführbar sein. Das heißt, die bisherige DP-Software und Teile der DP-Server Infrastruktur müssen vermutlich über die komplette Aufbewahrungsfrist der betroffenen Backups in Teilen weiter betrieben werden.
- Eventuell findet man auch einen Service-Provider, die abzulösende DP-Software betreibt und Restores als Dienstleistung anbietet.

### 6.1.4 Falls man den Storage-Hersteller nach NDMP-Backups wechseln will

**NDMP-Backups** sind Storage-Hersteller-proprietär. Daher sind diese evtl. für Restores über halbmanuelle Methoden (auch nach DP-Software-Wechsel) geeignet – aber nur, wenn zumindest die Kataloginformationen über den Beginn und Fortsetzung auf den Tape-Medien zur Verfügung stehen (Bandnummer, Tape-Marks, Fortsetzung auf anderen Medien, etc). Will man dagegen das benutzte Storage-OS wechseln, muss für NDMP-Restores ein Storage-System des bisherigen Anbieters für die komplette Aufbewahrungsfrist gehalten werden, von welchem der Backup einst erfolgte (teilweise genügen hier virtualisierte Storage-Systeme).

Eventuell findet man auch einen Service-Provider, der NDMP-Restores als Dienstleistung anbietet.

### 6.1.5 Public Cloud/SP vs. Eigenbetrieb (inklusive Private Cloud)

**Allgemeine Fragen beim Einsatz von Public Cloud-Diensten (Service-Providern)**

Die Nutzung von BaaS Cloud/SP-Diensten vs private Cloud vs traditionellem Inhouse-Lösungen erwägen

- **Vor dem Einsatz von Cloud-Speichern für das Backup sind folgende datenschutzrechtliche Aspekte abzuwägen (gesetzliche Vorschriften siehe Anlage; als auch Unternehmensinterne Abwägungen):**
  - Ist die Speicherung von Daten außerhalb der Unternehmens-Firewall bzw. außerhalb von Staatengrenzen grundsätzlich zulässig?

- Interne Richtlinien
- Wie früh und wo müssen Daten verschlüsselt sein?
  - Auf dem Transportweg
  - Beim Cloud-Speicher
  - Oder schon, bevor die Daten Richtung Cloud-Provider auf den Weg gegeben werden?
- Ist das Key-Management sicher genug und DR-Ready?
- Welche Verfügbarkeit und Performance Zusagen garantiert der Cloud Provider und sind diese mit den Anforderungen vereinbar? Sind die Zusagen nachprüfbar (z. B. durch Audits oder regelmäßige Tests)?
- Frühzeitige Einbindung des Datenschutzbeauftragten

- **Wie hoch sind die Gesamtkosten** (inkl. WAN-Traffic und zur Abdeckung des Wachstums)?

- **Was würde ein Providerwechsel bedeuten** (Daten-Umzug, Daten-Vernichtung, Kosten für das Auslesen der Daten, usw.)?

- **In welcher Form werden die Daten vom bisherigen Provider beim Wechsel zur Verfügung gestellt?** Gerade bei der Langzeitspeicherung von Backups müssen die Daten in einer Form übergeben werden, die vom neuen Provider weiterhin verarbeitet werden können, um nicht in ungewollte Abhängigkeiten zu geraten (Vendor lock-in).

### Nutzung von Public Cloud-Speichern nur für Backup/Restore/Disaster-Recovery

- **Ergeben sich Unterschiede bei der Erfüllung der Backup/Restore SLAs?** Wie sieht insbesondere der Restore-Fall aus? Welche Single Points of Failure (SPOF) bestehen (z. B. ist der lokale Cache-Speicher im Gateway zur Cloud redundant)?

- **Ergeben sich Unterschiede bei Disaster-Recovery Szenarien?** Backup in die Cloud kann bezüglich Disaster Sicherheit ein Vorteil sein, besonders wenn die Cloud-Daten-Kopie zusätzlich zum lokalen Backup erzeugt wird.

- **Fast immer ist beim Wechsel zum Backup to Cloud (B2C) die Disaster-Strategie zu überarbeiten.** Im Vordergrund steht dabei die Art und Weise, wie die Daten und die notwendigen Restore-Ressourcen zeitnah am Disaster Standort (könnten auch Cloud-Dienste sein) zur Verfügung stehen können.

### Backup/Restore/Disaster-Recovery, falls Primärdaten in der public Cloud liegen

- **Wer ist für Backup / Restore / Disasterrecovery zuständig?** Verantwortung komplett beim Cloud-Provider vs. Mix aus Eigenverantwortlichkeit und Cloud-Provider(n)?

- **Werden die eigenen Anforderungen bei der Erfüllung der Backup/Restore SLAs erfüllt?** Ist eine Überprüfung der Zusagen möglich, z. B. durch Audits?

- **Werden die eigenen Anforderungen bei Disaster-Recovery Szenarien erfüllt?**
  Ist eine Überprüfung der Zusagen (z. B. durch Disaster Tests) möglich? Ist eine Trennung in Brandabschnitte zwischen Primären Daten und Backups sichergestellt?

- **Falls die verwendeten Techniken der Cloud-Provider nicht offengelegt werden: Hält man die versprochenen SLAs und Schadenersatzklauseln für ausreichend?**
  Risikoanalyse zur Sicherstellung des Geschäftsbetriebes

- **Ist das Verlagern der Backup-Medien an einen anderen Standort, zu einem anderen Cloud-Provider oder zum Inhouse-Rechenzentrum aus Risikoabwägungen sinnvoll**
  (logischer/physischer Medienbruch und Brandabschnitt-Trennung)?

### 6.1.6 RZ-Infrastruktur / Backup Brandabschnitte / Desaster-Standorte überprüfen

Änderungen bei der Struktur der Backup Brandabschnitte und Disaster-Standorte erwägen

- Im Hauptstandort einen eigenen Backup-Brandabschnitt halten?
  - für alle Arten von Backup-Medien und alle Backup-Server?

- Kleinere Zweigniederlassungen in die Hauptniederlassung sichern?

- Falls ein eigener sicher getrennter Backup/DR-Brandabschnitt teilweise nicht sinnvoll/möglich ist:
  - wegen der physische Rahmenbedingungen (nur eine Firmen-Niederlassung)
  - weil es bei weit entfernten Zweigniederlassungen an lokalem IT Skill/Personal fehlt
  - aufgrund nicht darstellbarer Kosten für das weitere RZ (Klimatisierung/Notstrom/Netzzugang)

- dann sind andere Optionen auf Nutzbarkeit zu prüfen:
  - Anmietung von RZ-Flächen bei Housing-Providern, falls sich eigene Standorte nicht eignen.
  - Backup in die Cloud erwägen?
  - Medienauslagerung an einen sicher getrennten Ort

- Konsolidierung der Backup-Infrastruktur, damit weniger RZ-Fläche und –Ressourcen erforderlich sind?

Änderungen bei der technischen Infrastruktur jedes RZ erwägen

- Automatisches Stromlosschalten von Racks oder kompletten kleinen RZ ist (wenn andere Brandlasten außer der IT selbst entfernt sind) meist sinnvoller als eine CO2-Flutung.

- Bei CO2-Flutungsanlagen darauf achten, dass keine pneumatischen Signalhörner die HDDs gefährden (z. B. durch Einsatz elektronischer Hörner).

- Überspannungsabschottung (gegen Blitzschlag und starke Stromschwankungen) durch passende USV-Anlagen?

- Lohnen sich Notstromaggregate für länger andauernde Stromausfälle?

Änderungen bei der IT-Infrastruktur innerhalb der RZ erwägen

- Z. B. Virtualisierung von physischen Servern, auch um moderne Backup-Verfahren und Disaster-Recovery-Methoden anwenden zu können. Meist können zumindest Zweigstellen oder kleinere Standorte komplett mit virtualisierter Infrastruktur ausgestattet werden.

### 6.1.7 Nutzung von Tape als Backup-Medium?

Neben den Hinweisen zur Nutzung von Tape in Kapitel 5.1 sind noch folgende Punkte zu berücksichtigen:

- Umstellung auf eine 3rd oder 4th Generation DP-Methode (siehe Kapitel 3), falls dies ein sofortiges Backup in sicher entfernte Brandabschnitte ermöglicht?

- Tape-Auslagerung an einen DR-Standort abschaffen?
  - So können Security-Risiken während des Transports oder im Offline-Standort vermieden werden, falls keine Tape-Hochverschlüsselung verwendet wird.
  - Senkung von Prozesskosten und Minimierung von manuellen Fehlerquellen (inkl. Vertretungsregelungen).
  - Durch frühzeitigen online-Transfer der Backups in sicher genug entfernte Brandabschnitte (sofern die DP-Methode dafür effizient genug arbeitet) kann der Datenverlust bei DR drastisch verringert werden.

- Backup(2Disk)2Cloud (siehe 5.4) statt Backup(2Disk)2Tape sinnvoll?
  - Backup in die Cloud ermöglicht die Datenspeicherung in entfernte Standorte. Allerdings sind Performance und Kosten (besonders bei Langzeitspeicherung) genau zu prüfen. Für Tape sprechen weiterhin die hohe Streaming-Performance und die geringen Speicherkosten.

- Sofern Tape weiterhin sinnvoll ist:
  - Beschränkung der Verwendung von physischen Tapes auf einen zentralen Backup-Brandabschnitt?
  - Ist die Tape-Auslagerung verzichtbar (weil z. B. eine zweite Backup-Kopie vorhanden ist)?
  - Sollte der Zugang zum Tape-Roboter und Tape-Auslagerungsraum auf wenige Mitarbeiter beschränkt und/oder nur noch im 4-Augen-Prinzip ermöglicht werden?
  - Macht der Einsatz einer PBBA (Purpose Build Backup Appliance – siehe Kapitel 5.4.2) mit Tape im Backend Sinn?

### 6.1.8 Andere Abwägungen zur Optimierung

DP&R-Hardware/Methoden Änderungen erwägen

Hierbei können die beschriebenen Trends aus dem Kapiteln 4 und 5 Anregungen geben.

### 6.1.9 Vereinfachung von Backup-/Recovery- und DR-Prozessen erwägen

- **Ein generisches Backup-Scheduling kann den Aufwand und die Risiken minimieren** (Default Backup-Policy für Nicht-definiertes, Backup-Regeln auf Datastore-Ebene statt auf VM-Ebene, u.s.w.)
- **Endbenutzer/Applikations-Zuständigen Self-Service erwägen** (Restore-Prozesse, teilweise Backup-Prozesse)
- Zyklische **Recovery-Test**s (zumindest für Geschäftskritisches, wenn möglich automatisiert)
- **Vereinfachung von Failover und Failback-Prozessen**
- **mehr Automatisierung**

### 6.1.10 Lifecycle Management für Medien, Hardware und Software

- **Zyklische Backup-Medien-Überprüfung** (vor allem sehr alter Backupstände) auf technische Lesbarkeit
- **Medientausch-/Tape-Policy** (z. B. Tape-Refresh-/Migrations-Automatismen bei Langzeitspeicherung)
- **Sichere Medienlöschung/-Zerstörung** (falls nicht stark encrypted) vor Verlassen des Unternehmens
- **Wartungs- und Supportverträge überprüfen**
- **Lizenzierungs-Verifikation**

### 6.1.11 Validierung von Entscheidungen

Alle Änderungsüberlegungen sind von den jeweilig Verantwortlichen zu beurteilen bzw. zu evaluieren. Hierzu sollte man bei Bedarf zusätzlich entsprechende Fachkompetenz Dritter hinzuzuziehen.

Bei Unsicherheiten und/oder sehr hohem Folgeinvestment sollte ein Proof of Concept (PoC) durchgeführt werden, welches die entsprechenden Erkenntnisse vor einer produktiven Umsetzung erbringt.

### 6.1.12 Datenklassen, DP&R SLAs hinterfragen

- **Datenklassifizierung und Datenklassen definieren/bestehende hinterfragen**:
  Mit den Ergebnissen aus den Assessments lässt sich eine Datenklassifizierung durchführen, denen dann im Laufe der Maßnahmenabwägung ggf. veränderte Betriebs-SLAs für die Produktionsumgebung, Backup-SLAs, Restore-SLAs und DR-SLAs zugeordnet werden können.

- **DP&R SLAs definieren/bestehende hinterfragen:** DP&R SLAs sollten innerhalb eines Unternehmens nicht als auf Dauer fixiert verstanden werden. Sofern neue DP&R-Techniken deutlich mehr leisten können und sich diese für wesentliche Daten rechnet, sollten die SLA-Zusagen verbessert werden. Umgekehrt sollten nur mit extrem hohen Kosten erreichbare SLAs durch Herunterstufung vermieden werden. Meist ist eine (je nach IT-Größe) 2- bis 4-stufige Datenklassifizierung mit unterschiedlichen SLAs sinnvoll, da sich nicht für alle Daten die höheren DP&R-Investitionen rechnen.

  - Es erscheint sinnvoll, Kostensätze je GB (per SLA bzw. Datenklasse) zu (re-)kalkulieren und auszuweisen.

  - Besonders nach wesentlichen Änderungen sollten die betroffenen Zuordnungen überprüft werden.

## 6.2 Change Management / Umsetzung der Änderungen

### 6.2.1 Grundsätzliches zum Change Management

Veränderungen der aktuellen IT-Infrastrukturen müssen sorgfältig geplant, dokumentiert und in Abstimmung mit allen Beteiligten umgesetzt werden, damit negative Auswirkungen auf den Geschäftsbetrieb so gering wie möglich gehalten werden. Auch DP&R-Infrastrukturen können bei Betriebsstillstand negative Auswirkungen für den IT-Produktivbetrieb haben, wenn beispielweise Logdateien von Datenbanken nicht regelmäßig vom Produktivsystem weggesichert werden. Die DP&R-HW/SW-Infrastruktur besitzt Schnittstellen zu (fast) allen produktiven Systemen und Anwendungen (z. B. Backup-Agenten), was es beim Rollout von Änderungen zu berücksichtigen gilt. Derartige Gründe sprechen klar dafür, dass für die DP&R-Aspekte/Workflows Change Management Prozesse gegeben oder eingeführt werden sollten. Diese sind oft mit anderen IT Change-Prozessen verknüpft. Dabei sind nicht nur Änderungen der HW/SW-Infrastruktur zu berücksichtigen, sondern auch Betriebsänderungen oder Änderungen des

DP&R-Konzeptes selbst (z. B. Änderung von Ansprechpartnern). Fast bei jedem Change sollte man sich am Ende die Frage stellen, ob die Disaster-Readiness durch die Änderungen negativ tangiert sein könnte.

Für größere IT-Bereiche dürften ITIL-basierte Change Management Prozesse sehr sinnvoll sein – kleine IT-Abteilungen können ähnliche Prozesse evtl. auch ohne ITIL und eine unterstützende Software dafür umsetzen.

In ITIL (IT Infrastructure Library) sorgt der dort beschriebene Change Management Prozess dafür, dass Änderungsanforderungen geordnet gesammelt und nachvollziehbar umgesetzt werden. Dies sollte die Basis des DP&R- bzw. unternehmensweiten Change Prozesses sein – und wird mit steigender Anzahl der Beteiligten zunehmend essentiell. Auch der Detailierungsgrad sollte bei vielen Beteiligten entsprechend höher ausfallen.

Jeder Beteiligte kann Änderungen initiieren, z. B. IT-Hersteller durch neue HW/SW-Releases.

### 6.2.2 Produktive Umsetzung

Nach der Genehmigung der Änderungen beginnt die Planung und Implementierung der produktiven Umsetzung. Um nicht vorhersehbaren Komplikationen präventiv zu begegnen, empfiehlt es sich Fall-back Szenarien/Lösungen als Vorsorge zu definieren und/oder einen RollOut in mehreren Stufen anzustreben.

Eine lückenlose Dokumentation der Änderung, des Änderungsverlaufs und des Abschlusstests können von großer Wichtigkeit sein. Sollten direkt nach der Änderung oder im späteren Verlauf Probleme auftreten, ist diese Dokumentation wesentlich zur Durchführung der Fehleranalyse.

Damit die Änderungen und deren Auswirkungen auch bei allen betroffenen Abteilungen registriert werden, ist eine Kommunikation in geeigneter Form notwendig. Bei der Planung von Änderungen sollte auch immer ein notwendiger Schulungs- und Ausbildungsbedarf erwogen und ggf. eingeplant werden.

Auch wenn DP&R-Änderungen über zentrale Change-Prozesse dokumentiert wurden ist es empfehlenswert, das DP&R-Konzept aktuell zu halten (ggf. um Links in die zentralen Change-Management-Systeme zu ergänzen).

## 6.3 DP&R Betriebskonzept

Der Inhalt eines DP&R Betriebskonzeptes oder auch Betriebshandbuch hängt in Größe und Form natürlich von den spezifischen Gegebenheiten des Unternehmens ab.

Es dokumentiert die DP&R Umgebung und alle für den Betrieb notwendigen Festlegungen und Einstellungen.

Folgende Dokumentationen sollten Teil des DP&R-Betriebskonzeptes sein:

- **Beschreibung der Hardware-Installation**
  (Systeme, Komponenten, Verkabelung, Einstellungen, ...)
- **Beschreibung der Software-Installationen**
  (Lizenzen, SW-Module, Konfigurationen, Schedules, Scripts, ...)
- **Beschreibung der relevanten Betriebsprozesse**
  (Prozessinhalt, Monitoring, Zuständigkeiten, Change Management, Problem Management, Wartung, Reporting, Notfallvorsorge, spezifische Vereinbarungen, ...)

Mit den Informationen aus dem DP&R-Betriebskonzept sollte fachlich geschultes Personal umgehen können. Insofern ist es notwendig den Ausbildungsstand des Betriebspersonals bzw. externer Dienstleister entsprechend der Anforderungen aus dem DP&R-Betriebskonzept zu verifizieren.

### 6.3.1 Beispielgliederung eines DP&R-Betriebskonzeptes

Der folgende Grundsatz sollte für DP&R Betriebskonzepte erwogen werden: Wenig Abweichung von Standard-Betriebskonzepten spart aufwändige Dokumentation und Schulung.

Die folgende Gliederung zeigt beispielhaft den Aufbau eines DP&R-Betriebskonzeptes, an welchem viele Mitarbeiter/Funktionen beteiligt sind:

1. Dokumenten Information, Dokumenten Historie, Verteilerliste, ...
2. Übersicht Projekt-/Prozessziele, Dokumentenbestandteile
3. Verweis auf Basis Dokumentationen / Konzepte
4. Beschreibung der DP&R-Infrastruktur (Hardware, Netze, Backup-Software, Lizenzübersicht)
5. Betrieb der DP&R-Infrastruktur (Hardware, Netze, Backup-Software, Scripts, Prozesse, Zeitpläne, SLAs, ...)
6. Detail-Beschreibungen einzelner Komponenten (Konfiguration, Anpassungen, Prozeduren, ...)
7. Detail-Beschreibungen aller Backup-Methoden
   (Anwendungsabhängigkeiten, Einstellungen, GUI, CLI, ...)

8. Detail-Beschreibungen aller Restore-Methoden (Anwendungsabhängigkeiten, Einstellungen, GUI, CLI, ...)
9. Detail-Beschreibung des Backups und Restores der DP&R-Infrastruktur (GUI, CLI), inkl. Bare Metal Recovery
10. Wartungsarbeiten (Auswertung von Log-Dateien, Health-Checks, System / DP&R-Infrastruktur / Datacenter Shutdown, DON'Ts, ...)
11. Monitoring
12. Incident Management
13. Reporting
14. Disaster Handbuch, Wiederanlauf von Datacenter / DP&R-Infrastruktur / Systemen (siehe 6.4)
15. Change Management (Release Updates und Patches, Dokumentation, Knowledge Base, Downloads, Kompatibilitäten, Late Breaking News)
16. Spezifische Ergänzungen des jeweiligen IT-Betriebes
17. Datenschutzrechtliche Anforderungen und deren Umsetzung im DP&R Konzept (siehe auch Anlage)

### 6.3.2 DP&R Rechte

Zur Durchführung der Data Protection und Recovery Aufgaben sind einige Berechtigungen für die unterschiedlichsten Bereiche erforderlich. Diese Notwendigkeit sollte mit den Bedürfnissen an die Datensicherheit und den Datenschutz abgewogen werden, wozu die folgenden Hinweise dienen.

Als erstes sollte festgelegt werden, wer Zugang zur Backup-/Restore-Infrastruktur bekommt. Dies betrifft im Wesentlichen:

- Physischer Zugang zu Räumlichkeiten oder zu Backup-Systemen bzw. Racks
- Logischer Zugang - Trennung der Admin-Rechte für Primärdaten und Backup-Daten
- Zugang zu Backup-Daten in der »Cloud« oder ausgelagerten Datenträgern
- Einführung einer Zugangsverwaltung
  - Dokumentation der Regularien und der Berechtigungen
  - Über Vertretungsregelungen sind geplante/ungeplante Abwesenheiten zu regeln
  - Im Falle von externen Mitarbeitern oder Mitarbeiterwechseln, sind Berechtigungen nach Ausscheiden zu löschen
  - Zugriffe externer Dienstleister (z. B. Wartungstechniker) nur in Begleitung eigenen Personals gestatten
  - Zugriff auf »Encryption-Schlüssel« im DR-Fall regeln, um verschlüsselte Daten lesen zu können (z. B. über Key-Management-Systeme)

Des Weiteren können Berechtigungskonzepte der eingesetzten Backupsysteme genutzt werden, um Zugriffe gemäß der jeweiligen Rolle der Mitarbeiter zu regeln.

- Rollenkonzepte innerhalb der Backup-Software nutzen (z. B. Admin, Operator, Viewer)
- Festlegung und Dokumentation der Berechtigungen für die DP&R-Ausführung (Backup-Agents benötigen Zugriffsrechte für Betriebssysteme/Dateisysteme)
- Restore-Rechte verwalten (ggf. inkl. Berechtigungen für Applikationen)
- Mögliche Integration in bestehenden Directory Strukturen (z. B. Active Directory)
- Generell sollte darauf geachtet werden, dass Passwörter in Intervallen geändert werden und bei Nutzung von Zertifikaten, diese auch regelmäßig erneuert werden.

Bei komplexeren IT-Umgebungen sind folgende Punkte erwägenswert:

- Rechte-Trennung zwischen Primärdaten Administration und Backup-Administration
- Rechte-Trennung durch unterschiedliche Berechtigungen innerhalb der DP&R-Prozess-Workflows durch Nutzung verschiedener Technologien (wie Snapshot-Backup, Asynchrone Kopien vom Primär-Disk-Speicher, Tape-Kopien, Externe Unternehmen, usw.)
- Anwendungsbezogene Sicherungen (Backup- bzw. Restore aus der Applikation heraus mit Schnittstellen zur Backup-Applikation)
- Die gesamte Backup-/Restore-Umgebung in interne Audits zur Informationssicherheit mit aufnehmen

### 6.3.3 Workflow von DP&R Prozessen

Die Synchronisierung von Betriebsabläufen ist von wesentlicher und zunehmender Bedeutung. In vielen Unternehmen werden feste Backup-Fenster immer seltener oder stehen nicht mehr zur Verfügung. Außerdem müssen verschiedenste Backup-Verfahren (z. B. Snapshot-Erstellung, Tape-Kopie-Erstellung, anwendungsintegrierte Verfahren) untereinander und mit dem Anwendungsbetrieb ausgesteuert werden. Dies umfasst dem kompletten Backup-Workflow von der Planung über Ablauf, Monitoring, Reporting und Alerting.

Die dazu verwendbaren Tools können in drei Kategorien eingeteilt werden:

- **Terminplanung-/Jobsteuerung-Tools innerhalb der Backup-Software:**
  Die meisten am Markt befindlichen Backup-Software-Lösungen beinhalten zumindest ein Terminplanungs-Tool. Umfangreiche Lösungen integrieren klassische Datensicherung,

SnapShot-basiertes Backup und Archivierung in einer einheitlichen Oberfläche. Sehr gut geeignet sind Tools, die komplette Workflows abbilden können (z. B. über eine grafische Oberfläche) und somit durch reproduzierbare Abläufe das Betriebspersonal unterstützen.

- **Externe Jobsteuerung-Tools, die Prozesse RZ-weit steuern:** Vor allem in größeren RZ-Umgebungen sind externe Jobsteuerung-Tools im Einsatz, die unter anderem auch zur Steuerung des Backup-Ablaufs eingesetzt werden. Wichtig ist, Konflikte zwischen Backupsoftware-interner und externer Steuerung zu vermeiden.

- **Kundenspezifische, meist Script-basierte Tools:** Durch die Möglichkeit sowohl Infrastrukturen als auch Backup-Tools über CLI (Command Line Interface) bedienen zu können, ist Scripting der Abläufe eine weitere Steuerungs-Option. Zu bedenken ist der erhebliche Entwicklungs-, Test-, Pflege- und Dokumentationsaufwand. Außerdem ist zu klären, ob entsprechende Ressourcen auch in Zukunft für die weitere Pflege zur Verfügung stehen.

Bei der Auswahl der am besten geeigneten Workflow-Lösung sind u. a. folgende Fragestellungen zu klären:

- Durch welche Tools erfolgt der Schedule?

- Sind die geplanten Tools kompatibel zu bereits im Einsatz befindlicher Software bzw. gibt es Kommunikationsschnittstellen?

- Wie wird das Monitoring bzw. die Vollständigkeits-/Erfolgsprüfung umgesetzt? Können Ergebnisse aggregiert und an übergeordnete Tools weitergeleitet werden?

- Erlauben die Tools (inkl. der Infrastruktur) asynchrone Ereignisse, wie Anforderung von Recoveries, ohne den Ablauf zu stören? Sind (falls notwendig) insbesondere auch Restore Self-Service Anforderungen von Fachabteilungen oder Endbenutzern möglich?

- Können weitere Betriebsprozesse (z. B. Anlage von Clients, Eskalationsprozesse) durch Einsatz des Tools automatisiert werden?

- Wie sieht das Reporting von automatisierten Abläufen aus?

- Welche Aufwände entstehen durch das Customizing bzw. Entwicklung von Workflows?

- Wie sieht die Fehlerbehandlung bei Workflow-Problemen aus? (z. B. automatisierte Wiederanlaufmöglichkeiten)

## 6.4 Disaster-Recovery-Handbuch

Disaster sind glücklicherweise sehr selten, aber leider nie auszuschließen. Eine ganzheitliche Vorsorge gegen Disaster schließt die Erstellung und Pflege einer Dokumentation in Sinne eines Disaster-Recovery-Handbuches ein. Durch die regelmäßigen Überprüfungen der Konzepte und Maßnahmen, die im Disaster-Recovery-Handbuch und weiteren Dokumenten beschrieben sind, bleibt die Vorsorge gegen Disaster auf einem aktuellen Stand.

Eine intensive Einbindung und Information der Geschäftsleitung ist unerlässlich, um geeignete Disaster-Recovery-Szenarien zu definieren und notwendigen Mittel und Ressourcen zu bekommen.

Im Disaster-Recovery-Handbuch sind die Prozesse und Handlungsanweisungen für den Disaster-Fall beschrieben. Es soll alle Informationen, Dokumente und Handlungsanweisungen enthalten, die für die Wiederstellung des IT-Betriebs erforderlich sind.

- Beschreiben der Organisation, die sich mit der Bewältigung des Disaster-Falls beschäftigt
- Dokumentation des Wiederanlaufs kritischer IT-Services
- Festlegungen für den Notbetrieb
- Umfang der Unterstützung von Kunden und Fachabteilungen
- Wiederherstellung ausgefallener IT-Services
  (z. B. detailliert Server- oder Storage-Disaster Recovery beschreiben)
- ...

Bei der Erstellung eines Disaster-Recovery-Handbuches sollten auch auf die Empfehlungen des BSI zur Erstellung von Notfallhandbüchern geachtet werden. Gemäß BSI besteht ein Notfallhandbuch in Hinblick auf die Fortführung der Geschäftsprozesse insbesondere aus folgenden Dokumenten:

- Geschäftsfortführungspläne – sie beschreiben die Handlungsschritte für die Wiederherstellung der Geschäftsprozesse nach Krisen und Notfällen, beispielsweise die Schritte zur Inbetriebnahme eines Ausweichrechenzentrums.
- Wiederanlaufpläne - sie beschreiben die Handlungsschritte für die Wiederherstellung oder den Wiederanlauf wichtiger Ressourcen, die Priorität, mit der diese Schritte erfolgen müssen sowie die zugehörigen Verantwortlichkeiten.
- Weitere Dokumente: Plan für die Sofortmaßnahmen, Krisenstabsleitfaden, Krisenkommunikationsplan

Zum Aufbau eines Notfallhandbuches und von Geschäftsfortführungsplänen hat das BSI im Anhang zum Standard 100-4 Mustergliederungen veröffentlicht.

Sollte es Software gestützt sein, so ist auf eine geeignete Infrastruktur zu achten, die im Disasterfall leicht zugänglich ist bzw. einfach und sicher wiederhergestellt werden kann – also durch ein Disaster nicht verloren gehen kann.

Wichtig dabei ist genau zu spezifizieren, wann ein Disaster vorliegt, um welche Disaster-Kategorie (z. B. Infrastrukturteil- oder Gesamtausfall, Virenbefall, usw.) es sich handelt und was bzw. wie wiederhergestellt werden soll. Dadurch wird es möglich, direkt den der Situation entsprechenden Disaster Recovery Prozess zu starten. Dabei sind die Verantwortlichkeiten und Zuständigkeiten eindeutig festzulegen sowie zu kommunizieren. Nur wenn alle Beteiligten durch regelmäßige Schulungen bzw. Unterweisungen die notwendigen Kenntnisse besitzen, können im meist sehr hektischen Disasterfall alle Aktionen koordiniert, zielgerecht und risikoarm durchgeführt werden.

Die Wiederherstellung von Servern und Daten ist dabei nur ein Teil des Prozesses. Grundsätzlich müssen vorher wieder RZ-Bedingungen (z. B. nach Umweltkatastrophen) hergestellt werden. Dies kann zum Beispiel durch Hochfahren eines eigenen Disaster-RZ Standortes, einer Container-Lösung oder die Nutzung einer Cloud-Infrastruktur erreicht werden. Dabei ist es sehr wichtig, dass in diesem Moment oder in einem definierten Zeitraum die notwendigen Ressourcen am Disaster-Standort zur Verfügung stehen. Dazu gehören neben der Infrastruktur vor allem auch das Vorhandensein der Daten in einem aktuellen und konsistenten Zustand (was das zeitnahe Auslagern der Backups oder gar synchrone Spiegelungen voraussetzt).

Aufgrund der oft hohen Verfügbarkeitsanforderungen an die geschäftsnotwendigen IT-Prozesse, kommen typischerweise Standby-Infrastrukturen zum Einsatz, die bereits durch laufende Updates über die wichtigen Datenbestände verfügen. In welcher Form die Daten dort vorliegen (z. B. primäre oder Backup-Daten), hängt ebenfalls von der zu tolerierenden Ausfallzeit ab.

Wie bereits erwähnt ist die Aktualität der Dokumentation und der Mitarbeiterkenntnisse ein wesentlicher Faktor für die erfolgreiche Durchführung der Disaster-Bewältigung. Durch regelmäßige Disaster-Tests sollten die Maßnahmen geübt und auf Wirksamkeit überprüft werden – ohne Disaster-Tests ist ein hohes Risiko gegeben, dass man im Disaster-Fall insgesamt oder in Teilen scheitern dürfte.

# Anlage

## Rechtliche Anforderungen

# Rechtliche Anforderungen

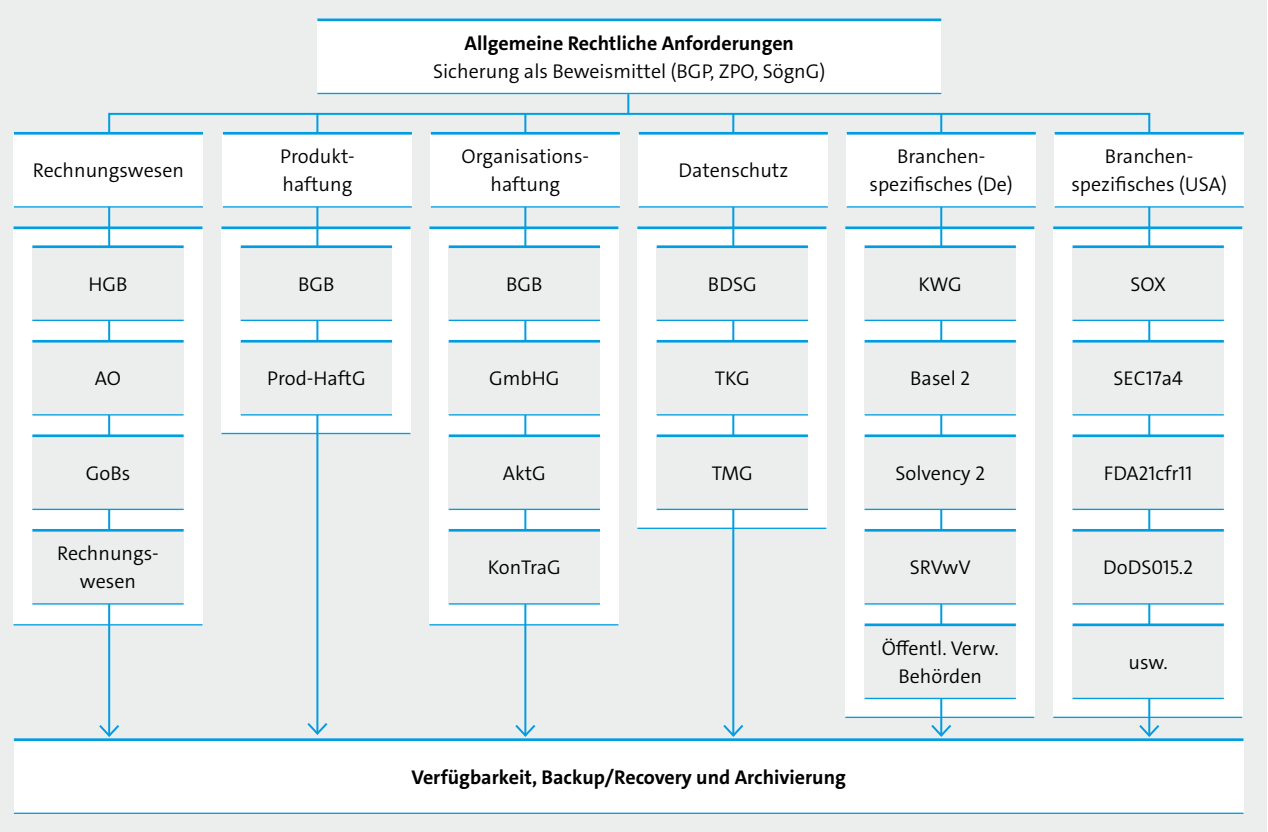
In diesem Kapitel wird auf die rechtlichen Anforderungen und Grundlagen für das Thema DP&R eingegangen. Das Kapitel wurde von einer Expertengruppe aus dem Arbeitskreis »Datenschutz« erstellt.

## Rechtliche Grundlagen

Für Backup & Disaster Recovery gelten zunächst dieselben rechtlichen Vorgaben wie für jede andere Datenverarbeitung. Deshalb muss derjenige, der ein Backup und Desaster Recovery Konzept erstellt, die enge Abstimmung mit der Rechtsabteilung, sowie den Compliance- und Datenschutzbeauftragten suchen. Das Backup und Disaster Recovery Konzept (DP&R Konzept – siehe Kapitel 6) muss rechtlich an der planmäßigen Datenverarbeitung orientiert werden. Das jeweilige betriebsinterne IT-Compliance-Konzept gibt die Maßnahmen zur Einhaltung der rechtsverbindlichen Mindestanforderungen in Bezug auf die Sicherheit und Verfügbarkeit von Informationen vor. Die Erstellung eines Backup erlaubt nicht, die für die ursprüngliche, planmäßige Datenverarbeitung und -speicherung maßgeblichen Vorgaben zu überschreiten.

Daher sollte grundsätzlich zwischen Archivierung und Backup / Desaster Recovery unterschieden werden. Es handelt sich um zwei unterschiedliche Ziele, die verfolgt werden. Ein Backup kann ein Archiv nicht ersetzen und ein Archiv kein Backup.

Während bei einem Backup die Wiederherstellung von Informationen bei einer Störung oder einem Datenverlust im Vordergrund steht, geht es bei der Archivierung um die Umsetzung der gesetzlichen Aufbewahrungspflichten einschließlich der damit einhergehenden Anforderungen an eine datenschutzkonforme Löschung von personenbezogenen Daten. Insbesondere die fristgerechte Löschung von personenbezogenen Daten ist bei einer Vermischung der beiden Zwecke sehr aufwendig. Datensicherungen, die über einen größeren Zeitraum aufbewahrt werden sollen, müssten regelmäßig auf zu löschende Daten geprüft und entsprechend bereinigt werden.




Quelle: EMC

Abbildung 18: Rechtliche Anforderungen

In der Praxis werden daher die gesetzlichen Aufbewahrungspflichten häufig in den operativen Systemen, in denen die Daten anfallen, umgesetzt (die Daten müssen dann nach Wegfall des ursprünglichen Zwecks innerhalb der Anwendung gesperrt werden) oder in einem separaten Archivierungssystem aufbewahrt. In solchen Archivierungs-systemen ist es dann möglich, die Daten bei Erreichen der gesetzlichen Aufbewahrungsfrist zu löschen.

In keinem Fall rechtfertigt die Notwendigkeit eines Backup und Desaster Recovery die Speicherung von personenbezogenen Daten über einen längeren Zeitraum, als dies für den Zweck der planmäßigen Datenverarbeitung erforderlich ist.

## Gesetzliche Anforderungen an die Speicherung von Daten

In unterschiedlichen Gesetzen finden sich Pflichten zur Aufbewahrung von Daten und entsprechende Fristen. Diese folgen typischerweise dem ursprünglichen Zweck der Datenverarbeitung. Deshalb sind die Aufbewahrungspflichten für den konkreten Einzelfall und in enger Abstimmung mit der Rechtsabteilung, sowie dem Compliance-Beauftragten zu ermitteln.

Folgende Anforderungen ergeben sich für die Aufbewahrung von Geschäftsdaten jeder Art, also nicht für personenbezogene Daten im Besonderen, weshalb sie typischerweise auch bei B&R Konzepten beachtet werden müssen. Die folgenden Anforderungen werden daher üblicherweise nicht durch die entsprechend lange Einlagerung von Datensicherungen umgesetzt, sondern durch ein abgestimmtes Backup- und ein Archivierungskonzept.

### §§ 146, 147 AO

Besondere Bedeutung haben die handels- und steuerrechtlichen Aufzeichnungs- und Buchführungspflichten gemäß §§ HGB § 238, HGB § 257 HGB sowie § AO 147 AO. Unternehmer als Kaufleute im Sinne des Handelsrechts müssen danach folgende Unterlagen aufbewahren: Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte, sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen; darüber hinaus auch die empfangenen Handelsbriefe, die Wiedergaben der abgesandten Handelsbriefe, sowie die Buchungsbelege. Aus dem Abgabenrecht ergibt sich zusätzlich die Aufbewahrungspflicht für sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind. Hierbei ist zudem zu beachten, dass eine Aufbewahrung außerhalb des Geltungsbereichs der AO – also außerhalb der Bundesrepublik Deutschland – mit dem zuständigen Finanzamt abzustimmen ist, § 146 Abs. 2a Satz 1 AO.

### GoBD

Zu berücksichtigen sind auch die Festlegungen in den »Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« (GoBD), die am 14.11.2014 verabschiedet wurden und in welchen die Akzeptanzgrenzen der Finanzverwaltung hinsichtlich der elektronischen Datenverarbeitung definiert werden. Dies betrifft insbesondere die Nachvollziehbarkeit und Nachprüfbarkeit sowie die Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung, die Vollständigkeit, Richtigkeit und Unveränderbarkeit der Aufzeichnungen.

Bitkom hat hierzu eine ↗Arbeitshilfe veröffentlicht.

# Datenschutzrechtliche Anforderungen an Backup und Desaster Recovery bei der Verarbeitung personenbezogener Daten

Das BDSG macht allgemeine Vorgaben zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die durch spezialgesetzliche Regelungen ergänzt werden. Diese Vorgaben sind grundsätzlich über alle Branchen hinweg und sowohl für jede planmäßige Datenverarbeitung, als auch für das Backup-Konzept und Desaster Recovery zu beachten.

## Datenschutzrechtliche Schutzmaßnahmen

Für personenbezogene Daten gibt es im BDSG als Anlage zu § 9 Vorgaben zu technischen und organisatorischen Schutzmaßnahmen:

a. Zutrittskontrolle: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

b. Zugangskontrolle: Die Nutzung von Datenverarbeitungssystemen durch Unbefugte ist zu verhindern.

c. Zugriffskontrolle: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

d. Weitergabekontrolle: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

e. Eingabekontrolle: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

f. Auftragskontrolle: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

g. Verfügbarkeitskontrolle: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

h. Trennungsgebot: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme bei der Zugangs-, Zugriffs- und Weitergabekontrolle ist nach dem Gesetzgeber insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Aus diesen Vorgaben sind bei Backup und Desaster Recovery-Überlegungen insbesondere die Vorgaben zur Weitergabekontrolle und Verfügbarkeitskontrolle zu beachten. Letztendlich sind Umsetzungen von Backup und Desaster Recovery-Maßnahmen auch Umsetzungen, die sich aus der Verfügbarkeitsanforderung des BDSG ergeben. Da sich Backup und Desaster Recovery-Überlegungen wie geschildert an der ursprünglichen, planmäßigen Datenverarbeitung orientieren müssen, sollte das jeweilige Backup und Desaster Recovery-Konzept eng und frühzeitig mit dem Datenschutzbeauftragten abgestimmt werden. Der Datenschutzbeauftragte überblickt die gelebte Praxis innerhalb des Unternehmens und kann Auskunft darüber geben, welche Vorgaben im Einzelnen beachtlich ist, beispielsweise hinsichtlich der betrieblichen Regelungen zur Nutzung privater Endgeräte (»Bring-your-own-device«), die Nutzung von Applikationen, oder die Einschaltung von Cloud-Anbietern und deren Zertifizierung.

## Einschaltung eines Dienstleisters

Sollte für das Backup und das Desaster Recovery von personenbezogenen Daten ein Dienstleister eingeschaltet werden, sind mit diesem die Anforderungen, die sich aus einer Auftragsdatenvereinbarung nach § 11 BDSG ergeben, zu vereinbaren.

Für Details hierzu wird auf den Bitkom ↗Leitfaden und die Mustervertragsanlage zur Auftragsdatenvereinbarung verwiesen.

Dort finden sich auch ausführlichere Angaben zu den Schutzmaßnahmen, sowie weitergehende Ausführungen zu den Überzeugungspflichten des Auftraggebers zur Einhaltung der vereinbarten Schutzmaßnahmen beim Auftragnehmer. Es empfiehlt sich, auch hier den betrieblichen Datenschutzbeauftragten in die Überlegungen und Ausgestaltungen einzubeziehen. Er klärt auch, inwieweit eine Vollverschlüsselung personenbezogener Daten nach Stand der Technik den Anwendungsbereich einer Auftragsdatenvereinbarung ausschließen kann (so beispielsweise das Bayerisches Landesamt für Datenschutzaufsicht, 6. Tätigkeitsbericht, Ziffer 5.2 zur Frage der Archivierung verschlüsselter Daten).

## Datenübermittlung ins Ausland

Erfolgt das Backup oder das Desaster Recovery mit personenbezogenen Daten im außereuropäischen Ausland, sind weitere Maßnahmen zu beachten.

Eine Datenübermittlung ins Nicht-EU-Ausland (»Drittlandtransfer«) ist nur dann rechtlich zulässig, wenn entweder eine Ausnahmeregelung für die konkrete Datenübermittlung vorliegt oder wenn ein angemessenes Datenschutzniveau im Sinne des § 4 Abs. 2 S. 2 BDSG sichergestellt wird.

Dies kann durch einen Angemessenheitsbeschluss der EU-Kommission nach Art. 25 Abs. 6 der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46 EG), durch die Verwendung von verbindlichen unternehmensinternen Reglungen (Binding Corporate Rules – BCR), die von einer Datenschutzaufsichtsbehörde freigegeben wurden oder der Verwendung seitens der EU-Kommission vorgegebenen Standardvertragsklauseln erfolgen. Hinsichtlich eines Datentransfers ins außereuropäische Ausland an einen Dienstleister ist zu beachten, dass die Binding Corporate Rules für Dienstleister gelten bzw. die Standardvertragsklauseln für Auftragsverarbeiter (Processors) eingesetzt werden.

Erfolgt das Backup oder das Desaster Recovery in den USA, sollte aufgrund der Entscheidung des EuGH vom 06.10.2015 durch den Datenschutzbeauftragten eine aktuelle Einschätzung der Zulässigkeit erfolgen.

## Zweckbindung

Hervorzuheben ist bei personenbezogenen Daten, dass diese dem Prinzip der Zweckbindung unterliegen, d. h. sie dürfen nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Der Zweck der Datenverarbeitung folgt aus der konkret zu erfüllenden Aufgabe und muss durch einen gesetzlichen Erlaubnistatbestand legitimiert sein. Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen zulässig.

Daten, die im Rahmen der Datensicherung gespeichert werden, unterliegen gemäß § 31 BDSG (oder einer vergleichbaren Regelung in den Datenschutzgesetzen der Bundesländer für den öffentlichen Bereich) zudem einer besonderen Zweckbindung, wenn sie ausschließlich zu Zwecken der Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden. So wurde in einem Fall entschieden, dass eine Sicherungsdatei über Emailverkehr, die im Rahmen einer Migration der technischen Infrastruktur erstellt wurde, auch später nicht mehr für Beweiszwecke in einem Strafverfahren verwendet werden durfte, nachdem die Originaldateien bereits gelöscht waren (VGH Mannheim, Urt. v. 30.7.2014 – 1 S 1352/13).

Doch die Grundsätze der Zweckbindung aus dem Datenschutzrecht wirken sich auch auf die Löschregelungen der gesicherten Daten aus: Für jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss eine rechtliche Grundlage vorliegen, die an einen Zweck gebunden ist (§ 4 Abs. 3 Nr. 2, § 28 Abs. 1 Satz 2 BDSG). Ist dieser Zweck erfüllt oder weggefallen, müssen die Daten grundsätzlich gelöscht werden (§ 35 Abs. 2 BDSG) bzw. durch Einschränkung von Berechtigungen in IT-Systemen gesperrt werden (§ 35 III BDSG). Zwar kann man die Daten im Backup kurzzeitig als »gesperrt« betrachten, jedoch setzt dies voraus, dass bei einer Wiederherstellung der Daten unverzüglich wieder eine Löschroutine über die Datensätze läuft, die nach dem Wiederherstellungspunkt bereits gelöscht wurden. Eine längere Aufbewahrung von Backups über mehrere Monate oder gar Jahre wird aber – sofern personenbezogene Daten enthalten sind – grundsätzlich nicht den gesetzlichen Löschverpflichtungen gerecht werden können.

## Konzept zur Löschung von Daten

Nicht nur für personenbezogene Daten ist es erforderlich die Speicherfristen zu definieren und im Sinne des Information Lifecycle Regeln für die Löschung der Daten zu implementieren. Wesentliche Elemente einer unternehmensweiten Lösung sind:

1. Systematische Erfassung und Klassifizierung der Datenarten hinsichtlich Verwendungszweck, Rechtsgrundlagen und Sensivität,

2. Festlegung von Standardlöschfristen entsprechend der Klassifizierung,

3. Technische Umsetzung der Löschregeln für die Standardlöschfristen.

Zur umfassenden Darstellung dieser methodischen Vorgehensweise sowie deren Umsetzung unter Mitwirkung aller fachlich und technisch zuständigen Bereiche wird verwiesen auf die

- DIN 66398 »Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten«.

Zu den technischen Möglichkeiten des Überschreibens oder Vernichtens von Datenträgern können zu Rate gezogen werden

- DIN 66399 »Vernichtung von Datenträgern« auf der Grundlage von Schutzbedarfsklassen und Sicherheitsstufen;

- Baustein B 1.15 des BSI-Grundschutzkatalogs »Löschen und Vernichten von Daten« mit den dort beschriebenen zugehörigen Maßnahmen.

# Glossar

verwendete Fachbegriffe mit kurzer Erklärung in alphabetischer Reihenfolge:

**AO (Abgabenordnung)**
Die Abgabenordnung (AO) ist das elementare Gesetz des ↗deutschen Steuerrechts. Da sich in ihr die grundlegenden und für alle ↗Steuerarten geltenden Regelungen über das Besteuerungsverfahren finden, wird sie auch als Steuergrundgesetz bezeichnet. Mehr unter ↗Abgabenordnung

**Assessment**
↗Technikfolgenabschätzung

**Backup (Datensicherung)**
Festhalten von Datenzuständen zum Zwecke eines evtl. notwendigen späteren Zurücksetzens (Restore). Typischerweise sollte ein Medienbruch und ein sicher getrennter anderer Brandabschnitt in einer Backup-Kette implementiert werden, um wesentliche Risiken zu minimieren.
Im allgemeinen Sprachgebrauch wird sowohl der Prozess des Erstellens einer Datensicherung als auch das Ergebnis als Backup bezeichnet.

**Bundesdatenschutzgesetz (BDSG)**
Das deutsche Bundesdatenschutzgesetz (BDSG) regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden. Mehr unter ↗Bundesdatenschutzgesetz

**Block Level Incremental (Forever)**
Nach einer initialen Vollsicherung der Blöcke werden in den darauffolgenden Backupläufen nur noch die geänderten Blöcke gesichert. Damit können die Backuplaufzeiten deutlich verkürzt werden. Mehr unter↗Backup

**BMR (=Bare Metal Recovery)**
Ist ein Server/Workstation Recovery-Verfahren das automatisch dieses System von Grund auf wiederherstellt, ohne die Erfordernis vorher Software oder das Betriebssystem zu installieren. Mehr unter ↗Recovery

**BYOD (Bring your own device)**
Bezeichnung für dienstliche Nutzung von privaten Geräten. Mehr unter↗BYOD

**B&R (=Backup und Recovery)**
Sicherung von Datenzuständen und Wiederherstellung der Daten und Dienste. Siehe dazu Kapitel 1.2 und auch die Beschreibung der Fachbegriffe »Backup« und »Recovery«.

**Changed Block Tracking (CBT)**
Ist eine Technologie, mit der man Block-inkrementelle Backups realisieren kann.

**Clone**
Eine Kopie eines vollständigen Datenzustandes zu einem bestimmten Zeitpunkt, welcher auch Schreibzugriffe erlauben kann. Im Zusammenhang mit snapshot-basiertem DP&R meist als differentieller Clone implementiert (nur die Veränderungen des Clones zum Basis-Snapshot belegt dann zusätzlichen Speicher). Mehr zu dieser Nutzanwendung im Kapitel 5.4 Snapshot.

**Cloud (Private/Public/Hybrid)**
Cloud (wörtlich »Wolke«) oder Cloud Computing bezeichnet ein IT-Modell, das weit über das reine Computing – also die Nutzung von Rechenleistung – hinausgeht. Es werden hier immer mehr standardisierte Cloud-Services angeboten, welche einfache bis komplexe IT-Funktionalitäten liefern können (z. B. nur ein Speicher, der für Backup-Zwecke genutzt wird oder einen kompletten Applikationsbetrieb mit integrierter Backup/Restore-Funktionalität). Ein Hauptaspekt der Cloud ist die Hochautomatisierung bei der Bereitstellung und des Betriebs der Cloud-Services. Ein anderer Hauptaspekt ist die Fähigkeit, die Services bei beliebigen dazu fähigen Dienstleistern zu betreiben (»Public Cloud« = Betrieb bei Dienstleistern – meist über das Internet-Netz; »Private Cloud« = Betrieb im eigenen Unternehmen; »Hybrid Cloud« = gemischter Betrieb mit eigenen und fremden Ressourcen). Mehr unter ↗Cloud

**Continuous Data Protection (CDP)**
Beschreibt ein Verfahren, bei dem eine kontinuierliche Datensicherung erfolgt. Ziel hierbei ist die Wiederherstellbarkeit von Daten auf einen beliebigen und nicht vorher definierten Zeitpunkt. Gesichert wird, sobald die zu sichernden Daten sich ändern.

**Converged Solutions / Converged Infrastructure**
Beschreibt eine »schlüsselfertige« IT Infrastruktur mit vorkonfigurierter Hardware- und Software für eine spezielle Aufgabe (z. B. Mailservice). Mehr unter ↗Searchdata und ↗Wikipedia

**Deduplication (=Deduplikation / Deduplizierung)**
Ist ein Datenreduktionsverfahren, welches zum Ziel hat, die zu speichernde Datenmenge verlustfrei zu reduzieren. Über eine Duplikat-Erkennung innerhalb möglichst großer Datenbestände werden mehrfach verwendete Datenelemente erkannt und durch Referenzen auf eine zentrale Speicherstelle eliminiert. Mehr dazu im Kapitel 5.3 und unter↗Wikipedia

**Differential Backup**
Bei der sogenannten differenziellen Sicherung werden alle Datenveränderungen, die seit der letzten Komplettsicherung aufgelaufen sind, gesichert. Da die differenzielle Sicherungsmenge mit jedem neuen Backuplauf steigt, wird in regelmäßigen Abständen eine neue Komplettsicherung erstellt und ein neuer Zyklus von differenziellen Sicherungen gestartet. Mehr unter ↗Differential Backup und ↗Differenzielle Sicherung

**DP (=Data Protection)**
Sicherung von Datenzuständen und Wiederherstellung der Daten und Dienste. Siehe dazu Kapitel 1.2 und auch die Beschreibung der Fachbegriffe »Backup« und »Recovery«.

**DP&R (=Data Protection und Recovery)**
Sicherung von Datenzuständen und Wiederherstellung der Daten und Dienste. Siehe dazu Kapitel 1.2 und auch die Beschreibung der Fachbegriffe »Backup« und »Recovery«.

**DPaaS (Data Protection as a Service)**
Typischerweise ein Cloud-Dienst, bei welchem die Datensicherung gänzlich oder teilweise an einen Dienstleister vergeben wird. Mehr unter ↗Wikibon und ↗Techopedia

**DRaaS (Disaster Recovery as a Service)**
Typischerweise ein Cloud-Dienst, bei welchem (oft als Ergänzung von DPaaS) im Falle eines Desasters die Systeme im Rechenzentrum des Dienstleisters wieder hergestellt werden bzw. auf dieses Rechenzentrum umgeschaltet wird.

**Ethernet**
Ein Protokoll für den Datentransport. Mehr unter ↗Wikipedia

**FCoE (Fibre Channel over Ethernet)**
Ein Protokoll für den Datentransport.

**Fibre Channel (FC)**
Ein Protokoll / Zugriffsart für Speichermedien.
Mehr unter ↗Wikipedia

**Flash**
Eine elektronische Speicher-Technologie, welche die Daten auch stromlos aufrechterhält. Meist wird »Flash« als Synonym für verschiedene Schaltungsarten von Storage-Class-Memory verwendet. Eine von mehreren anderen Schaltungsarten wäre PCM (Phase-Change-Memory). Die derzeit meist benützte Verbreitungsart sind SSDs (Solid State Disks), eine elektronische Emulation drehender Disks. Mehr unter ↗Wikipedia

**GoBD**
Die »Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« (GoBD) regeln die Aufbewahrung von handelsrechtlich und steuerrechtlich relevanten Daten und Dokumenten in elektronischer Form. Mehr unter ↗Wikipedia und Kapitel 7.2.2

**HGB**
Handelsgesetzbuch der BRD

**Hypervisor**
Eine Hardware-Abstraktionsschicht, die teilweise ein Betriebssystem (Operating System, OS) zum Ansprechen physischer Hardware beinhaltet. Es dient zur Virtualisierung von Servern in Form von Virtual Maschines (VMs), welche dadurch wesentlich hardwareunabhängiger und somit flexibler werden. Mehr unter ↗Wikipedia

**Image Level Backup**
Auch als Speicherabbildsicherung bezeichnet. Hierbei werden komplette Abbilder der Datenträger oder nur einer Partition (auf Blockebene) erstellt. Mehr unter ↗Wikipedia

**Incremental / Incremental-Forever Backup**
Bei der inkrementellen Sicherung werden immer nur die Dateien oder Teile von Dateien gespeichert, die seit der letzten inkrementellen oder Voll-Sicherung geändert wurden oder neu hinzugekommen sind. Es wird immer auf der vorangegangenen Sicherung aufgesetzt. Für eine vollständige Rücksicherung (Restore) müssen neben der Vollsicherung auch alle folgenden inkrementellen Sicherungen zurück gespielt werden. Um die Anzahl der benötigten Sicherungen im Restore-Fall gering zu halten, wird oft in regelmäßigen Abständen (z. B. einmal pro Woche) eine Vollsicherung durchgeführt. Beim »Incremental Forever« Backup-Verfahren hingegen benötigt es nur eine initiale Vollsicherung, gefolgt von inkrementellen Sicherungen. Die Nutzung von Metadaten ermöglicht es dabei, alle benötigten Elemente für einen Restore zu identifizieren. Mehr unter ↗Wikipedia und ↗Wikipedia

**iSCSI (Internet Small Computer System Interface)**
IP-basiertes Zugriffsprotokoll auf Block-Storage.
Mehr unter ↗Wikipedia

**LAN (=Local Area Network)**
Bezeichnet ein lokales Computer-Netzwerk zum Datenaustausch zwischen den darin befindlichen Komponenten.
Mehr unter ↗Wikipedia

**NAS (=Network Attached Storage)**
NAS-Systeme bezeichnen einfach zu verwaltende Dateiserver, welche man einsetzt, um ohne hohen Aufwand unabhängige zentrale Speicherkapazität in einem Rechnernetz mit einem Netzwerkprotokoll bereitzustellen. Mehr unter ↗Wikipedia

**NDMP (=Network Data Management Protocol)**
NDMP ist ein über eine Herstellervereinigung www.ndpmp.org standardisiertes Protokoll zur Steuerung von Backups/Restores unter Einbeziehung von Storage-Systemen. Es wird vor allem zur Beschleunigung von NAS (unstrukturierte Filedaten) Backups eingesetzt. Ausführlichere Details dazu im Kapitel 4.18 NDMP und unter ↗Wikipedia

**Objectstore**
Im Unterschied zu tabellenorientierten Datenbanken oder Filesystemen werden Informationen hier als einzelne Objekte verwaltet. Diese Speicherungsart basiert auf Ideen der objektorientierten Programmierung. Zu einem Objekt gehören dessen (zentrale) Beschreibung (Metadaten) und die dazugehörigen jeweiligen Dateninhalte, welche eindeutige Objekt-IDs besitzen. Über die Methoden werden i.d.R. auch Zugriffseinschränkungen und Ablageregeln (wie Anzahl zu haltender Kopien) beschrieben. Mehr unter ↗Wikipedia Object Store bzw. ↗Wikipedia Object Database

**Point-in-Time-Recovery**
Zurücksetzen eines ganzen Computersystems, einzelner oder mehrerer Dienste, eines einzelnen Datums oder mehrerer Daten, auf den Zeitpunkt eines Backups (Recovery Point). Eine Point-in-Time-Recovery umfasst typischerweise einen oder mehrere der folgenden Teilprozesse:

1. Restore der Sicherung (bei Datenbanken: der Datenbank- und Protokolldateien)
2. Herstellen der Konsistenz von unvollständig gespeicherten Transaktionen:
   a. auf Dateisystemebene ggf. durch eine automatisierte Dateisystemüberprüfung und Korrektur
   b. bei Datenbanken durch ein Transaction-Rollback auf den Transaktionsbeginn oder programmierte Synchronisationspunkte (Sync-Points)
3. ggf. Reaktivierung von Zugriffsdiensten

**Achtung:** die für Datenbanken üblichere Roll-Forward-Recovery umfasst zusätzliche Prozesse; siehe Fachbegriff dazu.

**Primärspeicher (Primary Storage)**
Der Speicher mit den aktiven Daten (im Gegensatz dazu ist ein Secondary Storage ein weiterer Speicher, welcher für Sicherungszwecke oder zur Disaster-Vorsorge vorgehalten wird).

**Purpose Build Backup Appliance (PBBA)**
Vorkonfiguriertes Computersystem, das entweder als reines Backup-to-Disk-Target für vorhandene Datensicherungsprodukte dient oder selbst eine Datensicherungslösung enthält. PBBAs gibt es in Ausprägungen mit Deduplizierungs- und Replikationsfunktionalitäten für verschiedene Zugriffsschnittstellen sowie für das Backup in die Cloud. Mehr dazu im späteren Kapitel 5.4

**RAID (=Redundant Array of Independent Disks)**
Ein RAID-System ist eine Zusammenschaltung mehrerer physischer Massenspeicher (üblicherweise Festplattenlaufwerke oder Solid-State-Drives). Dadurch kann der Datendurchsatz steigen. Das Hauptziel ist aber meist ein unterbrechungsfreier Betrieb bei Ausfall von Laufwerken pro Raid-Verbund. Mehr unter↗Wikipedia

**Recovery (Dienstwiederherstellung)**
Wiederherstellung von ausgefallenen Diensten (z. B. E-Mail-Dienst) oder Computersystemen, so dass diese wieder voll funktionsfähig zur Verfügung stehen. Eine Dienstwiederherstellung umfasst ggf. die Wiederherstellung der Infrastruktur, der Daten (Restore), Einspielen aufgezeichneter Änderungen (bei Rollforward-Recovery) und den Neustart der Dienste.

**Recovery Time / Recovery Time Objective (RTO)**
Die Recovery Time ist die Gesamtdauer einer Dienst-Wiederherstellung. Das Recovery Time Objective ist die Sollvorgabe, wie lange eine Recovery maximal dauern soll. Mehr unter ↗Wikipedia

**Recovery Point und Recovery Point Objective (RPO)**
Der Recovery Point beschreibt einen Wiederherstellungspunkt = ein Backup. Beim Recovery Point Objective handelt es sich um den Sollzeitraum, der maximal zwischen zwei Datensicherungen liegen soll. Der maximale Datenaktualitätsverlust ist das Delta zwischen 2 Recovery Points. Mehr unter ↗Wikipedia

**Restore (Datenwiederherstellung)**
Wiederherstellung von Daten von einem oder mehreren Datenträgern auf einen gewünschten Zeitpunkt (Recovery Point). Dies ist ein wesentlicher Teilschritt einer Recovery. Mehr unter ↗Wikipedia

**Retention Time (Aufbewahrungszeit)**
Beschreibt den Zeitraum, wie lange eine Information (Datensicherung) aufbewahrt werden und zur Wiederherstellung zur Verfügung stehen sollen (teilweise von gesetzlichen Vorgaben zur Aufbewahrungsfrist bestimmter Dokumente beeinflusst; siehe Kapitel 2.8. Dies kann ein kompletter Datenbestand (Full-Backup) oder auch eine einzelne Information (z. B. eine E-Mail) sein.

**ROI (=Return of Investment)**
Betriebswirtschaftliche Kennzahl zur Messung der Rendite einer Investition. Mehr unter ↗Wikipedia

**Roll-Forward-Recovery**
Relationale Datenbanken führen i.d.R. neben der DB selbst ein chronologisches Log aller DB-Veränderungen zum Zwecke einer kontinuierlichen Datensicherung. Dieses Log sollte regelmäßig abgesplittet (Log-Truncation) und vor Verlust (am besten mehrfach) gesichert werden. Eine Roll-Forward-Recovery umfasst folgende Teilprozesse:

1. Restore der DB-Sicherung
2. Lückenloses Wiedereinspielen aller im DB-Log festgehaltenen Veränderungen bis zum gewünschten Zeitpunkt.
3. unvollständig gespeicherte Transaktionen durch ein Transaction-Rollback auf einen konsistenten Zustand (Transaktionsbeginn oder programmierte Synchronisationspunkte) bringen. Dieser Prozess wird von DB-Systemen typischerweise bei jedem Anstarten automatisch durchgeführt.
4. Reaktivierung der DB-Zugriffsdienste

Eine Point-In-Time Recovery (siehe Fachbegriffserklärung dazu) würde dagegen nur den Prozess-Schritt 1, 3 und 4 ausführen (also die DB nicht auf einen beliebigen Zeitpunkt, sondern nur auf den Zeitpunkt der DB-Sicherung zurücksetzen).

Auch Schattendatenbanken basieren auf der Roll-Forward-Recovery-Technik – meist mit voreingestelltem mehrstündlichem Zeitversatz, was dann allerdings nur eine Recovery-Fähigkeit auf diese Zeitspanne begrenzt.

**SAN (=Storage Area Network)**
Ein Speichernetzwerk zur Vernetzung von Speichersystemen. Mehr unter ↗Wikipedia

**SAS (=Serial Attached SCSI)**
Computerschnittstelle bei Speichersystemen. Mehr unter ↗Wikipedia

**SCSI (Small Computer System Interface)**
Computerschnittstelle bei Speichersystemen. Mehr unter ↗Wikipedia

**Sekundärspeicher (=Secondary Storage)**
Eine zweite Speicherung von Daten in einem meist sicher entfernten Brandabschnitt. Dies wird teilweise auch als »Backup Speicher« bezeichnet und hat in der Regel eine Doppelfunktion:

1. Haltung der Backup-Stände und

2. die Möglichkeit der Aktivierung bei einem Disaster beim Primärspeicher

**Service-Level-Agreement (=SLA)**
SLA kann man ins Deutsche als Dienstgütevereinbarung (DGV) oder Dienstleistungsvereinbarung (DLV) übersetzen. Das SLA bezeichnet eine Vereinbarung bzw. die Schnittstelle zwischen ↗Auftraggeber und ↗Dienstleister für wiederkehrende Dienstleistungen. Ziel ist es, die Kontrollmöglichkeiten für den Auftraggeber transparent zu machen, indem zugesicherte Leistungseigenschaften wie etwa Leistungsumfang, Reaktionszeit und Schnelligkeit der Bearbeitung beschrieben werden. Wichtiger Bestandteil ist hierbei die Dienstgüte ↗Servicelevel, welche die vereinbarte Leistungsqualität beschreibt. Mehr unter ↗Wikipedia

**Snapshot**
Wörtlich »Schnappschuss«. In der IT verbergen sich dahinter Verfahren, welche in Sekundenschnelle beliebig große Datenbestände zum Zwecke der Datensicherung »einfrieren«.
Mehr dazu im Kapitel 5.4 »Snapshot-Differenzblock-Techniken« und unter ↗Wikipedia

**SSD (Solid State Disk)**
Siehe Fachbegriff »Flash« und mehr unter ↗Wikipedia

**Virtualisierung**
Nachbildung eines Hard- oder Software-»Objekts« durch ein ähnliches Objekt mit Hilfe einer Software-Schicht.
Mehr unter ↗Wikipedia

**VMs (=Virtual Machines)**
Virtualisierte Server
Mehr unter ↗Wikipedia

**VPN (=Virtual Private Network)**
Virtuelles privates (in sich geschlossenes) Kommunikationsnetz. Mehr unter ↗Wikipedia

**WAN (Wide Area Network)**
↗Rechnernetz, das sich über einen sehr großen geografischen Bereich erstreckt. Mehr unter ↗Wikipedia

**WebDAV (=Web-based Distributed Authoring and Versioning)**
Standard zur Bereitstellung von Dateien im Internet (z. B. zum Zugriff auf Online Speicher). Mehr unter ↗Wikipedia

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

**Bundesverband Informationswirtschaft,**
**Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin
**T** 030 27576-0
**F** 030 27576-400
bitkom@bitkom.org
**www.bitkom.org**

bitkom