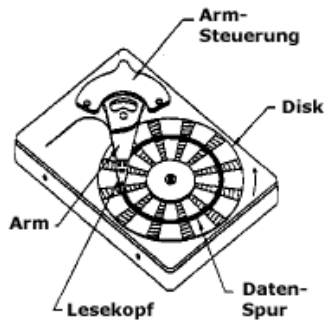


Information #001: Datensicherheit und Sicherungsstrukturen

Allgemeine Informationen:

Die wichtigste Aufgabe eines PC- oder Serversystems ist die sichere Bereitstellung und Aufbewahrung Ihrer Daten. Diese Aufgabe wird von Festplatten übernommen, welche die Daten speichern und bereitstellen. Festplatten sind Datenträger, welche die Daten auf konzentrisch übereinander gelagerten Scheiben magnetisch speichern. Ein Schreib- / Lesekopf wird zur jeweilig benötigten Stelle bewegt, damit die Daten durch Magnetisierung der Oberfläche gelesen und gespeichert werden können.



Ursachen für Datenverlust

Die Ursachen für einen Datenverlust können vielfältig sein. Die häufigsten Ursachen können in 3 Gruppen eingeteilt werden:

A) Verlust durch Hardwareschäden

Hardwareschäden sind ein häufiger Grund für Datenverlust. In den meisten Fällen sind Festplattenschäden der Grund für den Datenverlust. Festplatten sind mechanische Systeme und haben damit systembedingt nur eine begrenzte Haltbarkeit und unterliegen Verschleiß. Verschiedene Faktoren wie Verschmutzung, Stoßeinwirkung, Laufzeit und Temperatur (siehe unten), beeinflussen die Haltbarkeit von Festplattensystem maßgeblich. Ein solcher Schaden kann schleichend oder plötzlich auftreten. Zwar gibt es bei einigen Herstellern und Systemen die Option einer "Selbstprüfung" (S.M.A.R.T. Technologie), jedoch sollte man sich keineswegs auf diese Funktion verlassen. Die Daten von einer defekten Festplatte auszulesen ist sehr schwierig. In vielen Fällen können nur noch spezielle Firmen, welche auf Datenrückgewinnung spezialisiert sind oder der Hersteller selbst helfen, allerdings zu sehr hohen Kosten. Die einzigen Möglichkeiten, einen Datenverlust aufgrund von Festplattendefekten zu vermeiden, sind eine gute Auswahl der eingesetzten Festplatten, eine saubere Konfiguration und eine lückenlose Datensicherung. Auch eine neue Festplatte kann schnell Defekte aufweisen, das Alter eines Datenträgers lässt kaum Rückschlüsse auf die Zuverlässigkeit zu.

B) Verlust durch Softwarefehler und destruktive Software (Viren, Würmer, ...)

Auch eine fehlerhaft programmierte Software oder sehr häufig destruktive Software wie Viren können zu einem Ausfall des Serversystems oder zu Verlust von Daten führen. Ein Schutz vor Viren ist bei Beachtung wichtiger Sicherheitsmaßnahmen (siehe Infoblatt "Viren") relativ gut möglich, während Verluste durch Softwarefehler kaum vorhersehbar oder abwendbar sind. Wichtig ist hier eine engmaschige und schnelle Datensicherung, die auch schnell wiederhergestellt werden kann, da solche Fehler unvorhersehbar und unregelmäßig auftreten können.

C) Verlust durch den Benutzer (Fehlbedienung, Löschung, ...)

Fehler durch den Benutzer sind zwar grundsätzlich vermeidbar, aber dennoch durchaus als kritisch zu betrachten, da es kaum einen wirkungsvollen Schutz vor solchen Fehlern gibt. Auch ein perfekt abgesicherter Server kann kaum unterscheiden, ob die Löschung von Daten absichtlich oder versehentlich geschieht. Daher ist ein zeitversetztes Backup unbedingt notwendig, um die Daten eines bestimmten Zeitpunktes wiederzufinden. Dabei kann zwischen Löschung und Bemerkung des Fehlers durchaus eine längere Zeitspanne liegen, d.h. auch eine Archivierung der Sicherung ist ein wichtiger Schritt.

Die Wahl der richtigen Festplatte, Einflussgrößen auf die Datensicherheit

Auf dem Markt gibt es zahlreiche verschiedene Festplattenhersteller und -systeme. Dabei unterscheiden sich die Modelle hinsichtlich der Geschwindigkeit, aber auch hinsichtlich Interface-Typ und anderen Kenngrößen, die gerade für den Serverbetrieb wichtig sind.

Ein Desktop-PC hat dabei ganz andere Anforderungsprofile als ein Serversystem in einem Netzwerk. Desktop-PCs haben typischerweise 50 – 80 Lese-/Schreibzugriffe an 5 Tagen / Woche für ca. 8 Stunden pro Tag. Man spricht hier von einer Auslegung für 8x5 Stunden (8 Stunden je Tag bei 5 Tagen pro Woche). Ein Serversystem in einem mittleren Netzwerk führt dagegen z.B. an 7 Tagen pro Woche 24 Stunden am Tag Hunderttausende von Operationen aus.

Da Desktop-Festplatten einem hohen Kostenbewusstsein unterliegen, sind diese auch nur für ein beschränktes Belastungsprofil ausgelegt. Eine solche Festplatte sollte also nicht in einem Serversystem eingesetzt werden.

Ein ganz maßgeblicher Einflussfaktor, der für die meisten Festplattenschäden verantwortlich ist, ist die Temperatur der Festplatte. Die optimale Umgebungstemperatur für die meisten Festplatten sind 25° C. Erfahrungsgemäß liegen die Temperaturen der meisten ATA-Festplatten in PC-Systemen ohne besondere Maßnahmen zur Kühlung bei 50° C bis 55° C. Hierdurch sinkt die Lebensdauer erheblich, während die Ausfallwahrscheinlichkeit steigt.

Übliche Festplatten sind für eine Lebensdauer von 600.000 Betriebsstunden bei optimalen Bedingungen ausgelegt. Bei Temperaturen von 50° C sinkt diese Lebensdauer auf 200.000 Betriebsstunden ab. Dabei ist diese von den Herstellern angegebene Zahl nur von sehr theoretischer Bedeutung, da die Platten in der Realität deutlich höheren Belastungen ausgesetzt sind als dies in den Versuchsaufbauten der Fall ist.

Erfahrungsgemäß muss bei sicherheitsrelevanten Systemen von der Prämisse ausgegangen werden, dass die Festplatte schon im Neuzustand potentiell ausfallgefährdet ist.

Für Server-Systeme gibt es spezielle Festplatten, welche meist auf dem SCSI-Interface basieren und für höhere mechanische und thermische Belastungen ausgelegt, aber im Gegenzug auch deutlich teurer sind. Ob solche Festplatten für Ihr System geeignet bzw. empfehlenswert sind, kann und sollte im Einzelfall geprüft werden.

Unbedingt zu beachten ist – bei jedem Festplattentyp – eine suffiziente Kühlung, die auch in wärmerer Umgebung (kleine Räume, Sonneneinstrahlung, mehrere PCs in einem Raum, Rack-Einbau, ...) gewährleistet sein muss. Hierbei gibt es Varianten mit Luftkühlung (HDD-Lüfter, Einbaurahmen mit aktiver Belüftung, passive Aluminiumkühler, Heat-Pipes, ...) oder auch mit Wasserkühlung speziell für Festplattensysteme mit hoher Belastung.

Allgemeine Hinweise zur Datensicherung

Grundsätzlich kann man verschiedene Datensicherungsverfahren von einander unterscheiden:

- Manuell vs. Automatisiert

Ein manuelles Backup wird per Hand vom Benutzer aus gestartet oder zumindest bestätigt. Eine automatisierte Sicherung erfolgt selbstständig durch eine entsprechende Software oder hardwareseitig (s.u.).

- Full Backup vs. Inkrementelles Backup vs. Differentielles Backup

Ein Full Backup ist eine vollständige Sicherung von ausgewählten Daten. Bei dieser Sicherung werden alle Dateien des Verzeichnisses komplett kopiert, ungeachtet, ob diese schon zuvor gesichert wurden. Werden für das Full Backup wiederbeschreibbare Medien eingesetzt (Bänder, CD-RW, DVD-RW, ...), so werden diese vollständig überschrieben. Das Full Backup ist die einfachste, aber auch langsamste Form der Sicherung.

Bei einem inkrementellen Backup merkt sich die Sicherungssoftware, welche Dateien bereits gesichert wurden. So werden bei einem inkrementellen Backup nur die Dateien gesichert, welche sich seit dem letzten Backup geändert haben. Diese Form des Backups ist meist sehr schnell, da nur die geänderten Daten kopiert werden. Lediglich bei großen Datenbanken bietet sie keinen Geschwindigkeitsvorteil.

Ein differentielles Backup prüft alle geänderten Dateien im Vergleich zu einer Erstsicherung (z.B. einem Full Backup) und kopiert alle Daten, die zwischenzeitlich geändert oder erstellt wurden, auf das Backup-Medium. Zum Wiederherstellen der Sicherung ist also auch das erste (Full) Backup notwendig.

- Hardwaregestütztes Backup vs. Softwaregestütztes Backup

Bei einem Hardware-Backup, meist in Form eines RAID-Systems, wird die Datensicherung von einem Controller durchgeführt. Diese Lösungen sind meist weniger flexibel und kostspieliger, dafür jedoch deutlich schneller, weil sie das System nicht mit dem zusätzlichen Prozess der Datensicherung belasten. Hardwaregestützte Backups werden meist online, d.h. während des Betriebs, durchgeführt.

Ein Software-Backup wird durch eine Backup-Software durchgeführt, welche entweder permanent (online) im Hintergrund läuft oder zu einem bestimmten Termin (offline) die Daten auf ein Sicherungsmedium kopiert. Diese Lösungen sind preisgünstiger und bei bestimmten Formen der Sicherung prinzipbedingt notwendig (z.B. bei Sicherung auf CD/DVD), verlangsamen aber während der Sicherungstätigkeit das System spürbar.

- Online-Backup vs. Offline-Backup

Ein Online-Backup läuft permanent im Hintergrund und sichert eine Datei in dem Moment, in dem sie erstellt oder geändert wird. Damit ist die Sicherung stets sehr aktuell, jedoch anfälliger für Benutzerfehler (versehentliches Löschen oder Verändern einer Datei wird mitgesichert) und langsamer, da der PC / Server durch die Datensicherung einen zusätzlichen Prozess ausführen muss.

Ein Offline-Backup wird nur zu einer bestimmten Tageszeit durchgeführt, meistens in Arbeitspausen oder nach Beendigung der Arbeit, so dass die Verlangsamung des Systems nicht den betrieblichen Ablauf stört. Dieses Verfahren bietet eine höhere Toleranz bei versehentlichen Fehlern durch den Benutzer, im Schadensfall vor dem Zeitpunkt der Sicherung gehen die Daten bis zum Zeitraum der letzten durchgeführten Sicherung verloren.

Besonders wichtig im Rahmen einer Datensicherung ist nicht nur eine Server-interne Datensicherung, sondern auch die Sicherung auf ein mobiles, externes Medium, welches auch in regelmäßigen Abständen gesichert und vom Standort des Servers entfernt werden sollte, um eine Rekonstruktion des Datenbestandes bei Brand, Diebstahl oder Wasserschaden sicherzustellen.

Informationen über die Dauerbeständigkeit von Medien finden Sie weiter unten.

Übersicht über verschiedene Datensicherungssysteme im Server

A) RAID-Systeme

RAID-Systeme (redundante Anordnung unabhängiger Datenträger, definiert durch die Berkeley Universität, 1987) sind hardwareseitige Sicherungen, bei denen der Server die Daten auf mehrere Festplatte (je nach RAID Level) verteilt. Fällt eine der Festplatten aus, wird dies automatisch durch den RAID Controller kompensiert, der Betriebsablauf kann störungsfrei aufrecht erhalten werden. Bei professionellen System kann ein Austausch der defekten Festplatte bei laufendem Betrieb (hot swap) erfolgen, so dass keine Ausfallzeit durch den Defekt entsteht.

Übersicht RAID-Level:

<u>Level</u>	<u>Beschreibung</u>
0	<u>Striping</u> , d.h. mehrere kleine Laufwerke werden zu einem grossen logischen Laufwerk zusammengeschlossen. Dies erhöht die Geschwindigkeit, bringt aber keine Sicherheit.
1	<u>Mirroring</u> , d.h. zwei Festplatten werden mit den gleichen Daten beschrieben. Fällt eine Disk aus, wird die zweite eingesetzt. Das System ist jedoch etwas langsamer.
0+1, 10	Zwei Stripes (Level 0) werden zu einem Mirror (Level 1) zusammengefasst. Diese Konfiguration vereint die Sicherheit von Level 1 mit der Geschwindigkeit von Level 0, benötigt aber stets die doppelte Anzahl an Disks, sprich 4 Festplatten und ist damit recht teuer.
4	Besteht aus 3 Festplatten, wobei HDD 1 und HDD 2 die normalen Daten enthalten, während HDD 3 Prüfsummen in Form von Paritäten enthält, welche nach bestimmten Algorithmen die Daten verschlüsselt. Die Kapazität beträgt $(n-1) * \text{Plattenkapazität}$. RAID 4 wird heute nicht mehr angewendet.
5	Funktioniert wie RAID 4, jedoch werden die Paritäten auf alle Disks im System verteilt. Damit wird eine hohe Geschwindigkeit und eine gute Sicherheit garantiert, jedoch sind die Controller etwas teurer als einfache 0/1 Controller.

B) Wechselrahmen Festplatten

Müssen grosse Datenbestände schnell gesichert werden, so sind Festplatten immer noch die besten und günstigsten Medien zur Sicherung. So ist es beispielsweise möglich, Festplatten in herausnehmbaren (und abschließbaren) Wechselrahmen zu montieren, die zum Zwecke der Sicherung in den PC / Server eingeschoben sind und anschließend wieder entnommen. Der Vorteil ist eine schnelle Sicherung und eine sehr lange Aufbewahrungsdauer bei korrekter Lagerung der Festplatte.

C) CD-R(W) / DVD-R(W) Laufwerke

Optische Laufwerke setzen sich in den letzten Jahren immer mehr durch und sind mittlerweile der Standard in der Datensicherung, da die Medien günstig, weit verbreitet und einfach in der Handhabung sind. Es empfiehlt sich, für diese austauschbaren Medien einen Backup-Plan zu erstellen und für verschiedene Tage verschiedene Rohlinge zu verwenden. Über die Lagerung von den Rohlingen können kaum Aussagen getroffen werden, da sich die Qualität im Laufe der letzten Jahre stets geändert hat. Es ist jedoch davon auszugehen, dass eine CD-R Rohling kühl und trocken gelagert eine Haltbarkeit von ca. 10 Jahren erreichen sollte. CD-RW (wiederbeschreibbare) Rohlinge haben eine geringere Haltbarkeit, über DVD-R und DVD-RW Rohlinge liegen noch keine Langzeiterfahrungen vor. Die maximale Datensicherungskapazität liegt nach aktuellem Stand bei 8.4 GB / DVD Double Layer Rohling. Diese Medien eignen sich vor allem für eine Offline -Full-Backup Sicherung.

D) BMSD-Laufwerke

Die Thönissen EDV-Systeme BMSD (Backup Master Storage Device) Laufwerke sind externe Festplatten, die über die USB- oder FireWire-Schnittstelle angesteuert werden. Sie eignen sich hervorragend für eine differentielle oder inkrementelle Online- oder auch Offline-Datensicherung. Sie bieten zahlreiche Vorteile: Zum einen sind sie schnelle und große Datenspeicher, die auch eine lange und zuverlässige Haltbarkeit der Daten gewährleisten. Sie können leicht mitgenommen werden und außerhalb des Serversystems aufbewahrt werden. Darüber hinaus können Sie als Träger z.B. von Dateien und Datenbanken bei einem Serverausfall auch an andere Netzwerk-PCs angeschlossen werden und für einen definierten Zeitraum die Funktion einer (langsameren) Serverfestplatte übernehmen, d.h. sie sind nicht nur bei Festplattenschäden im Server, sondern auch bei anderen Hardwaredefekten eine sehr sinnvolle Ergänzung. Wahlweise sind sie im 5.25", 3.5" oder 2.5" Format erhältlich und damit auch als "Serverbackup im Hosentaschenformat" einsetzbar.

E) Bandlaufwerke

Die klassischen Bandlaufwerke verlieren zunehmend an Bedeutung, seit die optischen Laufwerke auch größeren Datenmengen sichern können. Nach wie vor bieten Bandlaufwerke den Vorteil einer großen Kapazität und einer sehr langen zuverlässigen Lagerungsdauer, die nach bisherigen Erkenntnissen unter guten Bedingungen über mehrere Jahrzehnte andauern kann. Damit eignen sie sich immer noch zur Archivierung von aufbewahrungspflichtigem Material. Nachteilig sind die hohen Anschaffungskosten sowie die langsame und laute Datensicherung. Eine Rekonstruktion von Daten durch Bandlaufwerke ist zeitintensiv und damit nicht im "Notfall" durchzuführen.

F) Weitere Möglichkeiten

Die o.g. Möglichkeiten sind die wichtigsten Backup-Methoden, die eine stabile Sicherung Ihrer Daten ermöglichen. Es gibt jedoch noch weitere Methoden, die hier kurz aufgezählt werden.

USB-Sticks bzw. Microdrives:

Ähnlich wie BMSD Laufwerke handelt es sich um externe Datenträger, welche über eine geringere Kapazität verfügen, dafür jedoch sehr klein und handlich sind und ideal als sicherer "Reisebegleiter" für sensible Daten geeignet sind.

Webserver:

Die Datensicherung erfolgt auf einem Server über das Internet, der auch an einem ganz anderen Ort stehen kann und sollte. Damit sind die Daten physikalisch unabhängig vom dem eigenen Betrieb / Netzwerk und können auch von anderen System und Orten abgerufen werden, z.B. zur Wartung und Pflege von Datenbeständen. Dem gegenüber steht eine vergleichsweise langsame Sicherung bei erhöhtem Sicherheitsrisiko für Ihre Daten. Ferner ist Webserver-Speicherplatz sehr teuer.

Andere PCs:

Wie bei einem Webserver können die Daten natürlich auch zu anderen PCs via Netzwerk oder Wireless LAN (Funknetz) übertragen werden, was durchaus auch eine sinnvolle Sicherungsform ist, da die Daten physikalisch auf einem anderen System liegen.

Die Backup Recovery CD / DVD – Datensicherung vs. Image

Die bisher angesprochenen Sicherungen sind reine Datensicherungen, d.h. Ihre Dokumente, Datenbanken und Dateien werden auf einem zweiten internen und / oder externen Datenträger gesichert. Bei einem Ausfall des Systems durch einen Festplattenschaden, durch einen Virus oder andere Beschädigungen kann es jedoch sein, dass nicht nur Ihre Daten, sondern auch das Betriebssystem (Windows, Linux, ...) und Anwendungsprogramme verloren gehen oder geschädigt werden. In diesem Falle muss bei einer Reparatur des Systems die Software neu aufgespielt werden, incl. aller notwendigen Einstellungen (Netzwerk, Kennwörter, Drucker, u.v.m.). Dies kann je nach System mehrere Stunden bis Tage dauern. Während dieser Zeit ist kein Server verfügbar, d.h. der Betrieb kann nicht fortgesetzt oder in gewohnter Form aufrecht erhalten werden.

Die Backup Recovery CD bzw. DVD von Thönissen EDV-Systeme enthält ein sogenanntes Image von Ihrer Festplatte. Dieses Image ist ein exaktes Abbild Ihrer Festplatte in komprimierter Form, welches auch Partitionsinformationen und den Bootsektor der Festplatte enthält. Im Falle eines Hardware-Schadens (Festplattendefekt) oder Softwareschadens (Virus, Bedienfehler, ..) kann so in wenigen Minuten (abhängig von der Größe der Festplatte) das System zum Zeitpunkt der Sicherung wiederhergestellt werden, d.h. der Server ist in kurzer Zeit wieder voll lauffähig.

Images sollten immer nach signifikanten Veränderungen an dem System (neues Softwareupdate, ...) erstellt werden, sind jedoch keine Lösung zur regelmäßigen Datensicherung. Die Erstellung und Rücksicherung eines Images sollte von Thönissen EDV-Systeme durchgeführt werden, eine fehlerhafte Benutzung der notwendigen Software kann zu Datenverlust führen. Ein Image ist jedoch die perfekte Ergänzung zu einer beständigen Datensicherung und garantiert schnellstmögliche Reparaturzeiten und damit geringe Ausfallzeiten.

Szenarien und Modelle von Datensicherungsstrukturen

Die Datensicherung ist eine der primären Aufgaben von PC- und Serversystemen. Dabei ist es nicht nur entscheidend, die Daten überhaupt gesichert zu haben, um sie im Falle eines Schadens wiederherzustellen, sondern je nach Struktur der EDV und je nach Betrieb ist auch der Zeitraum entscheidend, in dem ein PC- oder Serversystem wieder rekonstruiert ist, nachdem die Ausfallursache behoben ist.

PC-Speicheranwendungen

PC-Speicheranwendungen sind Bereiche, die bei einem Ausfall als weniger kritisch gelten, da in der Regel kein Produktions- oder Produktivitätsausfälle durch den Ausfall eines einzelnen PC entstehen, wenn dieser als reiner Terminal / Workstation eingesetzt wird. Die Anforderungen an die Festplatten sind eher gering, da sie weniger Schreib-/Leseoperationen und weniger Betriebsstunden ableisten müssen. Als Richtwert können 8x5 Stunden bei 260 Tagen / Jahr angenommen werden.

Sinnvoll ist die Erstellung einer Backup Recovery CD / DVD zu einem frühen Zeitpunkt der Rechnerinstallation, um zwangsläufige "Verunreinigungen" der Registry des Betriebssystems, wie sie fast immer typischerweise mit zunehmender Nutzungsdauer auftreten, zu vermeiden und ein möglichst "schlankes" System als Ausgangsbasis für die Wiederherstellung zu haben.

Die regelmäßige Sicherung kann in Form eines manuellen Full Offline Backups auf ein externes, meist optisches Datensicherungsmedium erfolgen, abhängig vom Zeitraum der Datenaktualisierung. Eine automatische Online Sicherung ist möglich, aufgrund der höheren Anforderungen an die Leistung des PCs bei geringerer Einschaltzeit jedoch meistens nicht empfehlenswert, sofern der Anwender "diszipliniert" genug ist.

RAID-Arrays oder Systeme mit mehreren magnetischen Datenträgern (Festplatten, Bandlaufwerke, BMSD-Laufwerke, ...) sind in PC-Systemen meistens schwieriger realisierbar, da Platzbedarf, Kühlung und Geräuschkulisse meistens limitierende Größen sind.

Empfehlung Konfiguration* und Datensicherungsverfahren* bei PC Speicheranwendungen

Harddisk	(S)ATA-Schnittstelle
Konfiguration Harddisk	Single Laufwerk, ggf. mehrere Partitionen
Kühlung	Keine, evtl. zusätzliche Luftkühlung
Laufgeräusch bei Tätigkeit	Typisch 2.5 bis 3.4 dB
Sicherungslaufwerke fest intern	Keine
Sicherungslaufwerke Wechseldatenträger intern	Optisches Laufwerk
Sicherungslaufwerke extern	Keine
Sicherungsmedien entfernbar	CD-R(W) / DVD-R(W)
Backup-Verfahren (empfohlen)	1. Backup Recovery CD / DVD
	2. manuelles Offline Backup auf CD / DVD
Backup-Verfahren (optional)	Keines
Zeitraum bis zur Wiederinbetriebnahme **	Mehrere Stunden bis ca. 1 Tag **

Nicht missionskritische Speicheranwendungen

Als "nicht missionskritische Anwendungen" werden nicht geschäftskritische Anwendungen bezeichnet. Diese können in der Regel wieder verwendet werden (z.B. medizinische Daten, digitale Röntgenbilder, archivierte Transaktionen, ...), werden jedoch nicht unbedingt sofort benötigt. Im Normalfall handelt es sich durch das stetige Anwachsen der Daten mit Archivierung der Datenbestände um große Dateimengen. Die Lebensdauer der Medien und deren Haltbarkeit sind entscheidender als die Performance. Die Betriebszeit wird mit 8x5 bis 24x7 kalkuliert.

Nicht missionskritische Speicheranwendungen sind in der Regel Datenbanken, welche auf einem Netzlaufwerk oder einem externen Datenträger gesichert werden und von dort abrufbar sein sollten. Eine sofortige Abrufbarkeit muss per definitionem nicht immer gewährleistet sein.

Die optimale Sicherungsform für nicht missionskritische Speicheranwendungen sind automatische differentielle oder inkrementelle Offline Backups auf externen Sicherungslaufwerken mit hoher Kapazität, so z.B. Bandlaufwerke oder auch BMSD-Laufwerke.

Bei Daten mit notwendiger oder verpflichteter Aufbewahrungspflicht über einen definierten Zeitraum ist eine Sicherung über Bandlaufwerke oder eine entsprechende Lagerung von CD-R / DVD-R Medien sinnvoll, welche in regelmäßigen Abständen geprüft und erneuert werden sollten.

Empfehlung Konfiguration* und Datensicherungsverfahren* bei nicht missionskritischen Speicheranwendungen

Harddisk	(S)ATA-Schnittstelle
Konfiguration Harddisk	Single Laufwerk, ggf. mehrere Partitionen Oder RAID 0 / 1 / 0+1
Kühlung	Passive oder aktive HDD Luftkühlung
Laufgeräusch bei Tätigkeit	Typisch 3.5 bis 5 dB
Sicherungslaufwerke fest intern	Keine
Sicherungslaufwerke Wechseldatenträger intern	Optisches Laufwerk, ggf. Bandlaufwerk
Sicherungslaufwerke extern	Ggf. BMSD Laufwerk
Sicherungsmedien entfernbar	CD-R(W) / DVD-R(W), Bänder (DAT)
Backup-Verfahren (empfohlen)	1. Full Backup in regelmäßigen Abständen 2. Backup auf lagerbaren Medien
Backup-Verfahren (optional)	Automatisches differentielles oder inkrementelles Offline Backup
Zeitraum bis zur Wiederinbetriebnahme **	Bis zu mehreren Tage **

Missionskritische Speicheranwendungen

Missionskritische Speicheranwendungen sind in der Regel mit vernetzter Server- und High-Density-Speicherung verbunden und betreffen Geschäftsbereiche wie Finanzwesen, Fertigung, Energie und Gesundheit, in denen es auf Geschwindigkeit, Genauigkeit, Datenverfügbarkeit und Zuverlässigkeit ankommt. Aufgrund der finanziellen und personellen Tragweite können bei diesen Anwendungen keine Ausfälle riskiert werden.

Der Ausfall eines Servers oder Systems, welches missionskritische Daten verwaltet ist per definitionem ein folgeschwerer Schadensfall durch Produktionsausfall oder Stillstand der Arbeitsprozesse bzw. Transaktionen. Neben einer effektiven und multidimensionalen Datensicherung steht somit auch die Absicherung vor Hardwareschäden durch Redundanz der Bauteile und eine Absicherung vor Stromausfällen und –schwankungen im Vordergrund eines Server-Managements.

Das erste Ziel in der Serverarchitektur ist die Vermeidung von Ausfällen durch entsprechend dimensionierte Datenspeicher, die auch für eine hohe mechanische und thermische Belastung ausgelegt sein müssen. Dabei wird grundsätzlich von einer garantierten Verfügbarkeit des Serversystems im Dauerbetrieb (24x7x365) ausgegangen. Da missionskritische Daten häufig auch einen laufenden Arbeitsprozess oder den Firmenbetrieb beeinflussen oder steuern, ist auch eine hohe Geschwindigkeit von hoher Bedeutung. Die Datensicherung sollte daher den Betrieb so minimal wie möglich beeinflussen.

Bei solch wichtigen Daten kann eine Sicherung nicht nur auf einem Wege bestritten werden, es muss stets eine langzeitstabile Sicherung auf einem externen Medium wie auch eine kurzfristig verfügbare Sicherung auf einem externen oder internen Medium angelegt werden. Als dritte Sicherheit sollten die Daten auf einem unabhängigen Redundanzsystem mit physikalischer Unabhängig zum Hauptsystem gelagert werden, um die Datenbankstruktur auch im größeren Schadensfalle am Hauptspeicher sofort verfügbar zu machen.

Ein entscheidender Schritt zum richtigen Fehlermanagement ist eine Ablauf- und Organisationskontrolle, bei der Ausfälle regelmäßig simuliert und die Backupsysteme auf ihre Integrität getestet werden. Auch Schulungen des Personals sind ein wichtiger Punkt für einen reibungslosen Ablauf im Falle eines Schadens.

Empfehlung Konfiguration* und Datensicherungsverfahren* bei missionskritischen Speicheranwendungen

Harddisk	(S)ATA-Schnittstelle möglich, empfohlen SCSI Schnittstelle
Konfiguration Harddisk	RAID-System Level 1 möglich, empfohlen RAID-System, Level 5
Kühlung	Aktive HDD Luft- oder Wasserkühlung
Laufgeräusch bei Tätigkeit	Typisch > 5 dB
Sicherungslaufwerke fest intern	Mindestens 1, empfohlen > 1
Sicherungslaufwerke Wechseldatenträger intern	Optisches Laufwerk, ggf. Bandlaufwerk Wechseldatenträger, gesichert
Sicherungslaufwerke extern	BMSD Laufwerk (ggf. mehrere)
Sicherungsmedien entfernbar	CD-R(W) / DVD-R(W), Bänder (DAT), BMSD transportabel (2.5" / 3.5" Format)
Backup-Verfahren (empfohlen)	1. Backup Recovery CD / DVD, mehrfach 2. automatisches Full Backup regelmäßig auf BMSD-Laufwerk 3. automatisches Full Backup regelmäßig auf externen Datenträger (DVD-RW) 4. automatisches inkrementelles Backup auf BMSD-Laufwerk 5. automatisches inkrementelles Backup auf externen Datenträger
Backup-Verfahren (optional)	Data-Warehouse, mehrere Systeme
Zeitraum bis zur Wiederinbetriebnahme **	Keine ungeplante Ausfalldauer

Einschätzung der eigenen Datenpriorität und Datensicherheit

In einem vorhanden System ist es für den Anwender häufig schwierig, die Qualität und die Zuverlässigkeit seines Systems und der installierten Datensicherheit abzuschätzen, zumal die Bewertung von Sicherheitslücken meist nur im Ernstfall bemerkt wird. Thönissen EDV-Systeme ist ein kompetenter Ansprechpartner bei Fragen und Systemlösungen für eine optimale, auf Ihre Bedürfnisse abgestimmte Datensicherungsstruktur. Wir analysieren Ihr System und simulieren auf Wunsch auch den "Ernstfall", um vorhandene technische Lösungen zu testen. Im folgenden sind einige Fragen gelistet, die uns oder auch Ihnen bei der Analyse Ihrer Systemstruktur behilflich ist.

1. Handelt es sich um ein Netzwerk mit Server oder um einen Einzelplatz-PC?

Netzwerksystem mit Server Peer-to-Peer Netzwerk Einzelplatz (☞ Punkt 4) unbekannt

2. Wie viele Arbeitsplätze sind in Ihrem Netzwerk integriert?

1-2 3-5 6-10 10-20 20-50 über 50 unbekannt

3. Welche Betriebssysteme werden auf den Arbeitsplätzen eingesetzt?

Microsoft Windows 9x/ME Microsoft Windows 2000/XP Linux anderes: _____ unbekannt

4. Welches Betriebssystem ist auf dem Server installiert?

Microsoft Windows 2000 / XP Microsoft Windows Server, Typ: NT 2000 2003 Linux unbekannt

5. Welche Festplattentechnik ist in Ihrem Server eingebaut?

1 Festplatte ATA 1 Festplatte SCSI RAID Array Level 1 RAID Array Level 5 unbekannt

6. Sind Komponenten des Serversystems redundant ausgelegt?

nein ja, Netzteil ja, Festplatten (RAID, s.o.) unbekannt

7. Über welche Datensicherungslaufwerke mit Wechselmedien verfügt der Server?

Bandlaufwerk CD-R(W) Laufwerk DVD-R(W) Laufwerk ZIP / JAZ o.ä. unbekannt

8. Verfügt der Server über eine Notstromversorgung?

nein ja, über eine Offline Online Hybrid unbekannt VA: _____ unbekannt

9. Wird der Server auch als Arbeitsplatz genutzt bzw. liegen die Daten auf einem Arbeitsplatz?

nein, der Server wird nur als Datenspeicher genutzt ja, der Server ist auch Arbeitsplatz unbekannt

10. Wie sind die Betriebszeiten des Servers?

ca. 8x5x300 ca. 8x5x365 ca. 24x5x300 ca. 24x5x365 ca. 24x7x300 ca. 24x7x365 unbekannt

11. Wie sind die Betriebszeiten Ihrer Firma / Praxis?

< 5 h / Tag 5 – 15 h / Tag > 15 h / Tag ganzjährig Saisonbetrieb unbekannt

12. Wie lange ist ein Ausfall der kompletten EDV im Tagesablauf tolerierbar?

mehrere Tage max. 48 h max. 24 h max. 5-10 h wenige Min. gar nicht!

13. Wie hoch wäre der organisatorische Aufwand in Ihrer Firma / Praxis, wenn die EDV ausfällt?

überschaubar mäßig hoch sehr hoch unbekannt

14. Entstehen finanzielle Schäden (Produktionsausfall, Transaktionen, ...) durch den Ausfall der EDV?

nein ja, tolerierbar ja, nicht tolerierbar ungefähr i.H.v. _____ unbekannt

15. Ist der Server selbst mit dem Internet verbunden?

nein ja, via analog / ISDN ja, via DSL, zeitweise ja, via DSL, permanent unbekannt

16. Sind die Arbeitsstationen mit dem Internet verbunden?

nein ja, via analog / ISDN ja, via DSL, zeitweise ja, via DSL, permanent unbekannt

17. Welche Backup-Formen werden derzeit von Ihnen eingesetzt (manuelle, automatisch, Full, differentiell, ...)

Dokumentation zur Datensicherung

Firma: _____ Standort: _____

Verantwortlicher Mitarbeiter: _____ nicht vorhanden

Datum der Dokumentationserstellung: _____

Einschätzung der Datenrelevanz:

keine PC-Speicheranwendung Nicht missionskritisch missionskritisch!

Informationen zur Server-Datenverwaltungsarchitektur

Single-HDD RAID-System Level 1 RAID-System Level 5 _____

Die zu sichernden Daten liegen auf folgenden Partionen / Teilbereichen / Verzeichnissen auf der Serverfestplatte:

- _____
- _____
- _____
- _____

Bei unzureichendem Platz bitte Rückseite verwenden.

Fortsetzung siehe Rückseite

Backup Recovery CD / DVD wurde(n) erstellt vom Server:

1. Partition C D ___ gesamter Datenträger bootfähig Anzahl: ___ CD DVD Datum: _____
2. Partition C D ___ gesamter Datenträger bootfähig Anzahl: ___ CD DVD Datum: _____
3. Partition C D ___ gesamter Datenträger bootfähig Anzahl: ___ CD DVD Datum: _____
4. Partition C D ___ gesamter Datenträger bootfähig Anzahl: ___ CD DVD Datum: _____

Backup Recovery CD / DVD wurde(n) erstellt von den Arbeitsplätzen:

Terminal 1 2 3 4 5 6 7 8 9 allen _____

Vorhandene eingesetzte Datensicherungslaufwerke:

Bandlaufwerk CD-R(W) Laufwerk DVD-R(W) Laufwerk BMSD-Laufwerk ZIP / JAZ _____

Backup-Dokumentation für die regelmäßige 1. Datensicherung Server (die o.g. Datenpfade):

manuelles Backup automatisches Backup

Offline um _____ Uhr an folgenden Wochentagen: Mo Die Mi Do Fr Sa So _____

Online hardwarebasiert softwarebasiert permanent Prüfung alle _____ Minuten _____

Full Backup Differentielles Backup Inkrementelles Backup _____

Auf Medium: Band CD-R CD-RW DVD-R DVD-RW BMSD-Laufwerk ZIP / JAZ _____

Backup-Dokumentation für die regelmäßige 2. Datensicherung Server (die o.g. Datenpfade):

keine 2. Sicherung

manuelles Backup automatisches Backup

Offline um _____ Uhr an folgenden Wochentagen: Mo Die Mi Do Fr Sa So _____

Online hardwarebasiert softwarebasiert permanent Prüfung alle _____ Minuten _____

Full Backup Differentielles Backup Inkrementelles Backup _____

Auf Medium: Band CD-R CD-RW DVD-R DVD-RW BMSD-Laufwerk ZIP / JAZ _____

Aufbewahrungsort Medien:

1. _____ 2. _____

Sonstige Hinweise:

Siehe Rückseite

Abschließende Hinweise in eigener Sache

(Anmerkungen zu * und **)

Eine falsch durchgeführte und fehlerhafte Datensicherung hat im Schadensfalle immer eine große Bedeutung, sei es einfach "nur" durch eine komplizierte und lang dauernde Wiederherstellungsprozedur, sei es durch einen Ausfall des Systems für einen längeren Zeitraum oder sei es im schlimmsten Falle durch den Verlust wichtiger und sensibler Daten, die unwiederbringlich verloren sind.

In unserer langjährigen Berufserfahrung im Umgang mit Netzwerksystemen haben wir häufig Sicherungssysteme erlebt, die nicht richtig durchdacht oder eingerichtet waren oder auch einfach nicht korrekt bedient wurden, und dabei auch festgestellt, dass die Kenntnis des Fehlers häufig zu spät um erst im Schadensfalle erfolgt.

Aus diesem Grunde haben wir diese Informationsseiten verfasst, um die korrekte Installation einer Datensicherung im Vorfeld aufzuzeigen und die verschiedenen Möglichkeiten zu erklären, die bei einer sinnvollen Datensicherung angebracht sind. Dabei muss natürlich immer von einer realistischen Einschätzung und Verhältnismäßigkeit ausgegangen werden, d.h. ein für manchen PC reicht das Kopieren von Dateien auf eine Diskette völlig aus, für andere Systeme ist aber eine aufwendige Sicherungsstruktur zwingend notwendig.

Die hier aufgezeigten Möglichkeiten und Empfehlungen sind allgemein und nicht immer für das individuelle Netzwerk übertragbar und beruhen auf unserer Einschätzung und Erfahrung. Eine für Sie ideale Backuplösung kann natürlich nur unter Kenntnis und Analyse der individuellen Begebenheiten in Ihrer Firma / Praxis realisiert werden.

Für eine solche Analyse oder Simulation eines "Ernstfalls" sowie weitergehende Beratung und Realisierung in verwandten Bereichen wie Notstromversorgung bis zu Wartungsverträgen stehen wir Ihnen gerne zur Verfügung.

Bitte beachten Sie jedoch, dass alle Angaben in diesem Informationsblatt ohne Gewähr sind und auch Druckfehler enthalten können, d.h. Thönissen EDV-Systeme kann nicht für Datenverlust haftbar gemacht werden, der in Folge von Empfehlungen oder Maßnahmen entstanden ist, die hier oder aufgrund dieses Informationsblattes genannt oder ergriffen wurden.

Die angegeben Zeiten, vor allem die zur Wiederherstellung, und Verfahren beziehen sich lediglich auf die Rückspielung einer effizienten Datensicherung nach Behebung des ursprünglichen Defektes. Die Behebung dieses Defektes kann, z.B. aufgrund von Ersatzteil-Lieferzeiten, erheblich länger dauern. Die Kompensation dieses Falles wird nur bei missionskritischen Systemen berücksichtigt. Die genannten Zeiten sind zudem ermittelte Erfahrungswerte von Thönissen EDV-Systeme, wobei Abweichungen nach oben und unten möglich ist und von den örtlichen Begebenheiten abhängen.

Eine Reparatur und Rekonstruktion eines Serversystems incl. seiner Datenbestände kann von Thönissen EDV-Systeme nicht in einer bestimmten Zeit garantiert werden, sofern darüber nicht eine gesonderte Vereinbarung, z.B. ein Wartungsvertrag, getroffen wurde.

Es gelten unsere Allgemeinen Geschäftsbedingungen.

Das Kopieren und die Weitergabe dieser Veröffentlichung an Dritte ist uneingeschränkt erlaubt, jedoch nur in Vollständigkeit und Originalität, d.h. es dürfen keine Informationen verändert, hinzugefügt oder weggelassen werden.