Datensicherung und Peripherie

KEIN BACKUP, KEINE GNADE!!!!!

Peripheriegeräte:

Bei der Auswahl eines geeigneten Datensicherungsmediums sollten verschiedene Faktoren berücksichtigt werden, darunter die Größe der zu sichernden Daten, die erforderliche Speicherkapazität, die Geschwindigkeit des Backups und der Wiederherstellung, die Kosten sowie die Anforderungen an Portabilität und Zugänglichkeit. Oftmals wird eine Kombination verschiedener Medien und Technologien verwendet, um ein ausgewogenes Verhältnis von Sicherheit, Kapazität und Effizienz zu erreichen.

- Externe Festplatten
  - Externe Festplatten sind beliebte Datensicherungsmedien aufgrund ihrer hohen Speicherkapazität, Portabilität und einfachen Handhabung. Sie werden über USB-, Thunderbolt- oder eSATA-Verbindungen mit einem Computer verbunden. Externe Festplatten können für regelmäßige Backups verwendet werden, indem sie manuell angeschlossen werden, oder sie können als Teil eines automatisierten Backup-Systems wie einer Netzwerkspeicherlösung (NAS) verwendet werden.
- Cloudspeicher
  - Cloud-Speicher hat in den letzten Jahren an Popularität gewonnen. Es handelt sich um virtuelle Speicherlösungen, bei denen die Daten auf entfernten Servern gespeichert werden, die über das Internet zugänglich sind. Cloud-Speicher bietet flexible Speicherkapazität, Skalierbarkeit und Fernzugriff auf die gesicherten Daten von verschiedenen Geräten aus. Beliebte Cloud-Speicheranbieter sind beispielsweise Dropbox, Google Drive, Microsoft OneDrive und Amazon S3.
- Netzwerkspeicher (NAS, DAS, SAN, Serverlösungen)
  - Netzwerkspeicher (NAS): NAS ist eine spezielle Art von Datenspeichergerät, das in ein Netzwerk integriert ist und mehreren Benutzern gleichzeitig Zugriff auf Daten ermöglicht. NAS-Systeme sind mit Festplatten bestückt und bieten erweiterte Funktionen wie RAID (Redundant Array of Independent Disks) für verbesserte Datensicherheit und -integrität. Sie können als zentrales Backup-Medium für mehrere Computer oder Server dienen und ermöglichen die automatisierte Durchführung von Backups über das Netzwerk.
- Bandlaufwerke
  - Bandlaufwerke waren lange Zeit ein gängiges Datensicherungsmedium, insbesondere für Unternehmen mit großen Datenmengen. Bandlaufwerke bieten hohe Speicherkapazität, Datendichte und eine lange Lebensdauer. Sie werden normalerweise für regelmäßige vollständige Backups verwendet, können aber auch für inkrementelle oder differentielle Backups eingesetzt werden. Die Wiederherstellung von Daten von Bändern kann jedoch im Vergleich zu anderen Medien zeitaufwändiger sein.
- Optische Speicher
  - CDs, DVDs und Blu-ray-Discs wurden früher häufig für die Datensicherung verwendet. Sie bieten eine geringere Speicherkapazität im Vergleich zu anderen Medien, werden aber immer noch in bestimmten Anwendungsfällen genutzt. Optische Medien eignen sich gut für die Archivierung von Daten, da sie eine langlebige Speicherlösung bieten, die vor physikalischer Beschädigung geschützt ist.

Allerdings erfordert die Verwendung optischer Medien häufig manuelle Handhabung und ist weniger praktisch für regelmäßige Backups.

Netzwerkspeicher:

DAS (Direct Attached Storage)

DAS bezieht sich auf Speichergeräte, die direkt an einen Computer angeschlossen werden, normalerweise über eine Hochgeschwindigkeitsverbindung wie USB, Thunderbolt oder eSATA. Bei DAS ist der Speicher direkt mit dem Host-Computer verbunden und steht diesem exklusiv zur Verfügung. Es kann sich um eine externe Festplatte, ein RAID-System oder eine andere Art von Speichergerät handeln. DAS bietet eine schnelle Datenübertragung, da es keine Netzwerklatenz gibt. Es eignet sich gut für den schnellen Zugriff auf große Datenmengen und Anwendungen, die hohe I/O-Leistung erfordern, wie beispielsweise Videobearbeitung. Jeder DAS-Speicher ist jedoch nur für den angeschlossenen Computer zugänglich und kann nicht von anderen Geräten über das Netzwerk genutzt werden.

- Direkt mit Host verbunden
- Hochleistungsverbindung
- Schnelle Datenübertragung, da keine Netzwerklatenz

NAS (Network Attached Storage)

NAS (Network Attached Storage): NAS ist ein eigenständiges Gerät, das über das Netzwerk mit Computern verbunden ist und als zentraler Speicherort für Dateien und Daten dient. Es verwendet ein Dateisystem, das den Datenzugriff über das Netzwerk ermöglicht, normalerweise über das Netzwerkprotokoll wie NFS (Network File System) oder SMB/CIFS (Server Message Block/Common Internet File System). NAS-Systeme sind in der Regel mit einem eigenen Betriebssystem ausgestattet und bieten erweiterte Funktionen wie Benutzerverwaltung, Zugriffskontrollen und oft auch zusätzliche Dienste wie Medienserver oder Cloud-Synchronisation.

- Eigenständiges Gerät
- Im Netzwerk für alle angebundenen Geräte verfügbar
- Eig. Betriebssystem
- Benutzer- und Zugriffsverwaltung
- Als Medienserver oder zur Cloud-syncronisation nutzbar
- Einfach zu installieren und konfigurieren / verwalten

SAN (Storage Area Network)

SAN ist eine Netzwerkarchitektur, die es mehreren Servern ermöglicht, auf gemeinsamen Speicher zuzugreifen. Es besteht aus einer Kombination von Switches, Host-Bus-Adaptern (HBAs) und Speichergeräten wie Festplatten-Arrays oder Bandbibliotheken. SAN verwendet spezielle Netzwerkprotokolle wie Fibre Channel oder iSCSI (Internet Small Computer System Interface), um eine hohe Bandbreite und geringe Latenz für den Speicherzugriff bereitzustellen.
Ein SAN ermöglicht es mehreren Servern, auf denselben Speicher zuzugreifen und ermöglicht Funktionen wie Failover, Lastverteilung und zentrale Verwaltung des Speichers. Es bietet auch erweiterte Funktionen wie Snapshotting, Replikation und Thin Provisioning. SANs werden häufig in großen Rechenzentren eingesetzt, in denen eine hohe Skalierbarkeit, Flexibilität und Leistung erforderlich sind.

- Eigenes Speicher-Netzwerk
- Kann von mehreren Servern zugegriffen werden
- Wird durch Switching Hot-Bus-Systemen oder anderen von Netzwerk getrennt und ist darüber mit Berechtigung erreichbar.
- Kombination aus versch. Festplatten-Arrays, Bandbibliotheken usw.
- Zusätzliche Funktionen wie: Failover, Lastverteilung, zentrale Verwaltung …

Der Hauptunterschied zwischen NAS, DAS und SAN liegt in der Art und Weise, wie der Speicherzugriff bereitgestellt wird. NAS ermöglicht den Dateizugriff über das Netzwerk, DAS bietet direkten Speicherzugriff für einzelne Computer und SAN ermöglicht den gemeinsamen Speicherzugriff über ein spezialisiertes Netzwerk. Die Wahl zwischen diesen Technologien hängt von den spezifischen Anforderungen des Systems, der Skalierbarkeit, der Leistung und der Datenzugriffsmuster ab.

System	Vorteile	Nachteile	Geeignet für
DAS	- Hohe Leistung und geringe Latenz	- Nur für den direkt angeschlossenen Computer	- Schneller Datenzugriff
	- Einfache Installation und Verwaltung	- Begrenzte Skalierbarkeit	- Anwendungen mit hoher I/O-Leistung
	- Exklusiver Zugriff auf den Speicher		
NAS	- Einfacher Dateizugriff über das Netzwerk	- Begrenzte Bandbreite	- Gemeinsamer Dateizugriff von verschiedenen Geräten und Betriebssystemen
	- Skalierbarkeit und Erweiterbarkeit	- Potenzielle Netzwerklatenz	- Datenspeicherung und gemeinsame Nutzung
	- Zusätzliche Funktionen (Benutzerverwaltung, Medienserver, etc.)		
SAN	- Hohe Bandbreite und geringe Latenz	- Komplexere Konfiguration	- Gemeinsamer Speicherzugriff für mehrere Server
	- Zentralisierte Speicherverwaltung	- Höhere Kosten	- Rechenzentren und große Umgebungen
	- Erweiterte Funktionen (Snapshotting, Replikation, etc.)		

Arbeitsauftrag:
Erstelle ein Backupsystem für ein Unternehmen.
Es soll monatlich ein Vollbackup gemacht werden und es sollen die Backups der letzten 6 Monate im Bestand bleiben. Das System soll für die kommenden 3 Jahre ausgelegt sein.
Der Datenbestand sind derzeit 180 TB. Der Datenzuwachs beträgt ca. 2 TB / Monat
Entscheide selbst, welche Peripheriegeräte benötigt werden, wie hoch der Speicherbedarf ist und welche Kosten ungefähr auf das Unternehmen zukommen.

Lösungsvorschlag:
180 TB
36*2 TB Zuwachs
252 TB Datenvolumen Am Ende der Zeit
252 +250+248+246+244+242
= 1482 TB Gesamtspeicherbedarf netto
Je Tape 30 TB (70,00€ je Band) → 54 Tapes (Vorhaltung 6 Monate je 9 Bänder)
Bandlaufwerk
Backupsystem mit 252 TB Nettospeicherkapazität →15 Platten á 18 TB → 260 TB + 36 TB Parität (2 Platten)

Daraus folgt:

- Backupserver mit 24 Einschüben ca. 3500,-
- 17 Festplatten á 18 TB HDD ca. 4500,-
- Bandlaufwerk min. 9 Tapes
- Server-Rack min. (HPE StoreEver MSL2024 0-Drive Tape Library mit 24x Slots - 407351-001 / AK379A ca. 700,-
-
- 54 Tapes á 30 TB ca. 3800,-
- Software und Zubehör ca. 800,-
- Switch ca. 250,-
    - 13.550,-
- Personalkosten 40 Std. á 120,-€ = 4800,-
    - **18350,-€ Gesamtkosten**

Backup

Backup-Arten:

- Vollbackup
- Differentielles Backup
- Inkrementelles Backup
- Mirroring Backup (Schattenlaufwerk)
- Image-Backup

Backup-Stratgien
Die Entwicklung und Implementierung von Backup-Strategien ist ein entscheidender Aspekt der Datensicherung. Hierbei geht es um die Festlegung, wie häufig Backups erstellt werden sollen, welche Daten gesichert werden müssen und welche Backup-Methoden angewendet werden sollen (z. B. Vollbackup, Differentielles Backup oder Inkrementelles Backup).
Generationenprinzip (Großvater-Vater-Sohn-Prinzip)
Siehe hierzu: Lernzusammenfassung LZ_004_Backup

RAID
(Redundant Array of independent Disks)

RAID ist eine Technologie, die es ermöglicht, mehrere physische Festplatten zu einem logischen Speicherarray zu kombinieren, um die Leistung, Zuverlässigkeit oder beides zu verbessern. RAID-Systeme bieten erhöhte Datenverfügbarkeit und -sicherheit durch Redundanz, indem sie die Daten auf mehrere Festplatten verteilen.

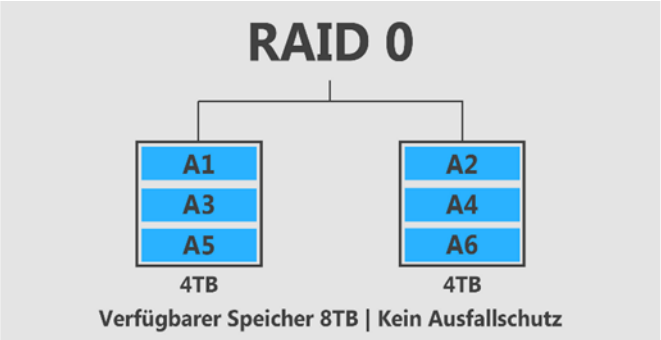
Es gibt verschiedene RAID-Level, die unterschiedliche Konfigurationen und Eigenschaften bieten. Die häufigsten RAID-Level sind:

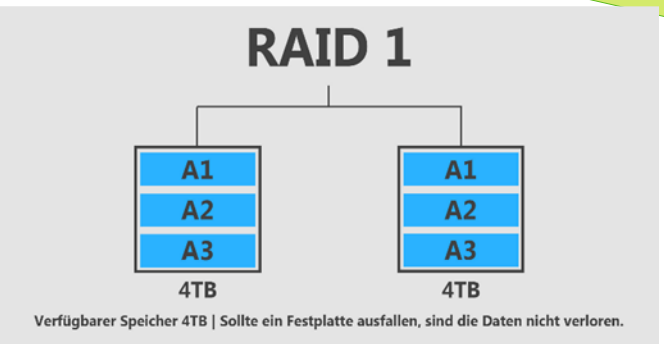
1. RAID 0 (Striping): RAID 0 verteilt die Daten gleichmäßig über zwei oder mehr Festplatten, um die Lese- und Schreibgeschwindigkeiten zu erhöhen. Es bietet jedoch keine Redundanz, da es keine Paritätsinformationen oder Spiegelung gibt. Das bedeutet, dass ein Ausfall einer Festplatte das gesamte Array beeinträchtigen würde, was zu einem vollständigen Datenverlust führen kann.
2. RAID 1 (Mirroring): RAID 1 verwendet Spiegelung, bei der die gleichen Daten auf zwei oder mehr Festplatten dupliziert werden. Wenn eine Festplatte ausfällt, sind die Daten immer noch auf den anderen Festplatten verfügbar, da sie identisch sind. RAID 1 bietet eine hohe Datensicherheit, aber die Kapazität wird halbiert, da die Hälfte der Festplatten nur als Spiegel für die andere Hälfte fungiert.
3. RAID 5 (Striping mit Parität): RAID 5 kombiniert Striping mit Paritätsinformationen, die auf den Festplatten verteilt werden. Wenn eine Festplatte ausfällt, können die Daten aus den verbleibenden Festplatten und den Paritätsinformationen wiederhergestellt werden. RAID 5 bietet eine gute Balance zwischen Leistung und Redundanz und verwendet die Kapazität einer Festplatte für Paritätsdaten. Es ist wichtig zu beachten, dass RAID 5 anfällig für den sogenannten "RAID 5 Parity RAID Penalty" ist, bei dem die Leistung während des Wiederaufbaus nach einem Festplattenausfall beeinträchtigt wird.
4. RAID 6 (Striping mit doppelter Parität): RAID 6 ist ähnlich wie RAID 5, jedoch mit doppelter Parität. Das bedeutet, dass RAID 6 den Ausfall von zwei Festplatten gleichzeitig verkraften kann, was die Datensicherheit erhöht. RAID 6 bietet eine bessere Redundanz als RAID 5, aber es benötigt auch mehr Festplatten für die Paritätsinformationen.

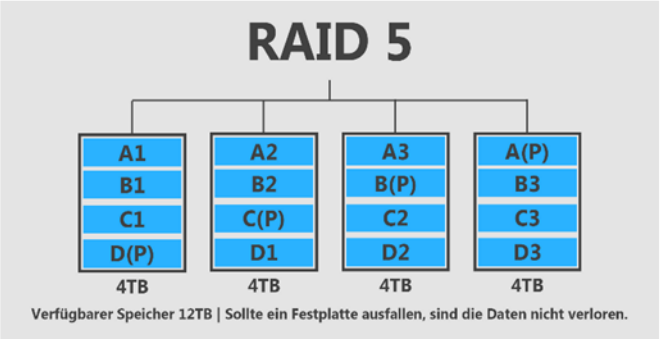
Es gibt auch weitere RAID-Level, wie zum Beispiel RAID 10 (RAID 1+0), das eine Kombination aus Spiegelung und Striping ist, um sowohl Leistung als auch Redundanz zu bieten. Die Auswahl des geeigneten RAID-Levels hängt von den spezifischen Anforderungen an Leistung, Kapazität und Datenredundanz ab.

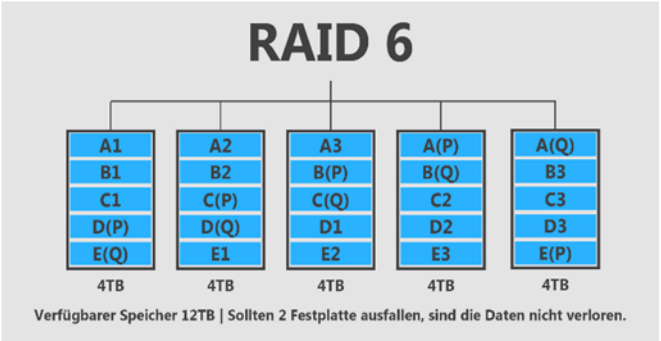
Übersicht der RAID-Level

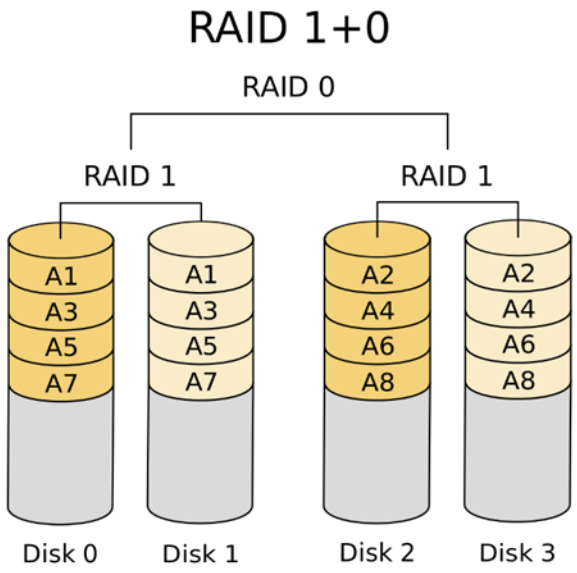
RAID-Level	Beschreibung
0	Striping, Stripe-Set 1 Zusammenfassung mehrerer Datenträger zu einem log. Laufwerk, keine Datenredundanz, dadurch schneller Datenzuqriff durch Erhöhung der Datentransferrate
1	Mirroring, Spiegelung1 mind. 2 HDD erforderlich, um sie zu spiegeln, Schreib- und Löschzugriffe werden automatisch auf die zweite HDD übertragen, 100 % Datenredundanz , jedoch viel ungenutzter Speicherplatz, da nur 50 % zur Verfügung stehen.
2	mind. 3 HDD, wie RAID 1 mit zweitem Controller zur Sicherheitserhöhung, Fehlerkorrekt. werden auf der weiteren Platte untergebracht, schnelle Rekonstruktion der Datenbestände, heute jedoch durch geringe Blockgrößen nicht mehr. aktuell
3	wie RAID 2 mit zusätzlichem Parity-Laufwerk für die Fehlerkorrekturen , leichter Anstieg der Plattenkapazitätsnutzung, 3 Platten (nur auf 1 und 2 Nutzdaten) , mittels der XOR-Verknüpfung können bei Plattenausfall die vorhandenen Daten r- mittelt werden, durch niedrige Blocklänge zwar schnelles Lesen, jedoch langsame Schreibvorgänge, heute nicht mehr aktuell
4	wie RAID 3 jedoch größere Blöcke (Erhöhung des Striping-Faktors)
5	mind. 3 Platten erforderlich, die Paritätsdaten sind auf sämtlichen gekoppelten Laufwerken (bis zu 32 Platten) verteilt , verbesserte Performance , da die Schreib- und Leseoperationen überlappt ablaufen können, hohe Datensicherheit mi einem hohen Datendurchsatz , eine Platte kann ausfallen , qeringere Kosten als RAID 2
6	wie RAID 5, aber mind. 4 Platten erforderlich , je nach Nutzdatenblock werden zwei Parity-Blöcke auf alle Laufwerke verteilt, bei Ausfall zweier HDD können die Daten wiederhergestellt werden, die Steuerungssoftware ist aufwendig
7	spezifische Erweiterung von RAID 6, die Parity-Daten werden auf einer separaten Festplatte abgespeichert, sehr aufwendige Lösung, sehr sicher und Verwaltung extrem großer Datenmengen, mehrere Rechner können gekoppelt werden, durch große Cache-Speicher in einer separaten Steuereinheit und asynchron. Betriebs jedes LWs mit eigenem Controller wird eine außergewöhnliche Sicherheit erreicht
10	[eins-null, nicht zehn] keine eigene Form, sondern Mischform aus 1 und 0, mind. 4 Platten erforderlich, die vorhanden Platten der Spiegelung (z. B. zwei RAID 1- Systeme) werden zum Stripeset kombiniert , um schnelle Datenzugriffe zu haben
01 0+1	null-eins oder null und eins] keine eigene Form, sondern Mischform aus 0 und 1,mind. 4 Platten erforderlich, das vorhandene Stripeset wird zur Datensicherheit gespiegelt
50	RAID 5-System als Stripeset
51	RAID 5-System gespiegelt (mindestens 6 Platten erforderlich)

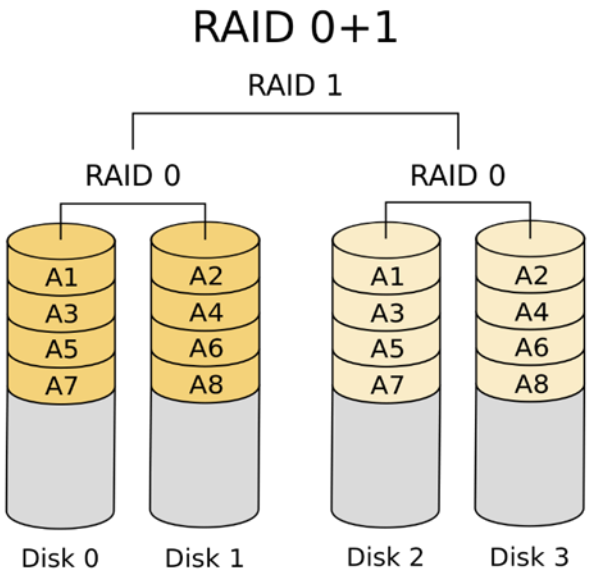

RAID 0
A1
A3
A5
A2
A4
A6
4TB
4TB
Verfügbarer Speicher 8TB | Kein Ausfallschutz

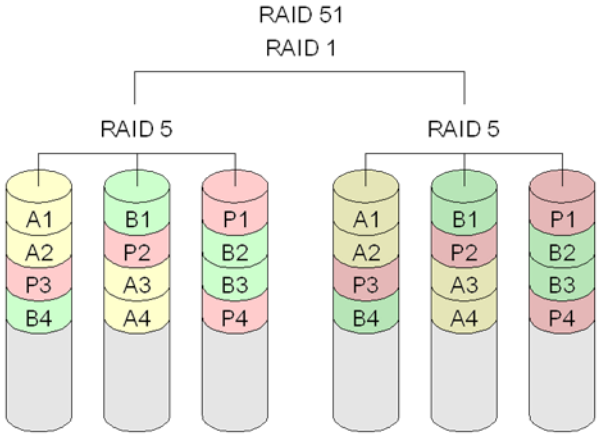

RAID 1
A1
A2
A3
A1
A2
A3
4TB
4TB
Verfügbarer Speicher 4TB | Sollte ein Festplatte ausfallen, sind die Daten nicht verloren.

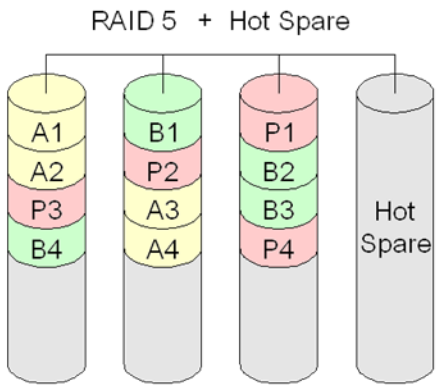

RAID 5
A1 B1 C1 D(P)
A2 B2 C(P) D1
A3 B(P) C2 D2
A(P) B3 C3 D3
4TB
4TB
4TB
4TB
Verfügbarer Speicher 12TB | Sollte ein Festplatte ausfallen, sind die Daten nicht verloren.


RAID 6
A1 B1 C1 D(P) E(Q)
A2 B2 C(P) D(Q) E1
A3 B(P) C(Q) D1 E2
A(P) B(Q) C2 D2 E3
A(Q) B3 C3 D3 E(P)
4TB
4TB
4TB
4TB
4TB
Verfügbarer Speicher 12TB | Sollten 2 Festplatte ausfallen, sind die Daten nicht verloren.


RAID 1+0
RAID 0
RAID 1
RAID 1
A1 A3 A5 A7
A1 A3 A5 A7
A2 A4 A6 A8
A2 A4 A6 A8
Disk 0
Disk 1
Disk 2
Disk 3


RAID 0+1
RAID 1
RAID 0
RAID 0
A1 A3 A5 A7
A2 A4 A6 A8
A1 A3 A5 A7
A2 A4 A6 A8
Disk 0
Disk 1
Disk 2
Disk 3


RAID 51
RAID 1
RAID 5
RAID 5
A1 A2 P3 B4
B1 P2 A3 A4
P1 B2 B3 P4
A1 A2 P3 B4
B1 P2 A3 A4
P1 B2 B3 P4


RAID 5 + Hot Spare
A1 A2 P3 B4
B1 P2 A3 A4
P1 B2 B3 P4
Hot Spare

Es ist wichtig zu beachten, dass RAID keine Ersatz für regelmäßige Backups ist. Obwohl RAID-Systeme vor Festplattenausfällen schützen können, sind sie nicht gegen andere Risiken wie Datenkorruption, Benutzerfehler oder Katastrophen abgesichert. Daher ist es empfehlenswert, regelmäßige Backups durchzuführen, um Datenverlust zu vermeiden.

Verschlüsselung

Verschlüsselung ist ein Prozess, bei dem Daten in eine unverständliche Form umgewandelt werden, um sie vor unbefugtem Zugriff zu schützen. Durch die Verwendung von Verschlüsselungstechniken können Daten in einen verschlüsselten Zustand gebracht werden, der nur mit einem speziellen Schlüssel oder Passwort wieder in ihren ursprünglichen Klartextzustand zurückversetzt werden kann. Hier sind einige wichtige Aspekte zur Verschlüsselung:

- Symmetrische Verschlüsselung: Bei der symmetrischen Verschlüsselung wird derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln von Daten verwendet. Der Sender und der Empfänger müssen über den gemeinsamen Schlüssel verfügen. Ein bekanntes Beispiel für eine symmetrische Verschlüsselung ist der Advanced Encryption Standard (AES). Symmetrische Verschlüsselungsalgorithmen sind in der Regel schneller als asymmetrische Algorithmen, aber die Herausforderung besteht darin, den gemeinsamen Schlüssel sicher zwischen Sender und Empfänger auszutauschen.

- Asymmetrische Verschlüsselung: Bei der asymmetrischen Verschlüsselung werden zwei unterschiedliche, aber mathematisch verwandte Schlüssel verwendet - ein öffentlicher Schlüssel zum Verschlüsseln der Daten und ein privater Schlüssel zum Entschlüsseln der Daten. Der öffentliche Schlüssel kann frei verteilt werden, während der private Schlüssel geheim gehalten werden muss. Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist der RSA-Algorithmus. Asymmetrische Verschlüsselung ist sicherer als symmetrische Verschlüsselung, erfordert jedoch mehr Rechenleistung und ist langsamer.

- Hash-Funktionen: Hash-Funktionen sind mathematische Algorithmen, die Daten in eine feste Zeichenfolge (Hash) umwandeln. Der Hauptzweck von Hash-Funktionen besteht darin, die Integrität von Daten zu gewährleisten. Bei der Verschlüsselung werden Hash-Funktionen verwendet, um den Hash-Wert einer Nachricht zu berechnen und diesen mit einem Signaturschlüssel zu verschlüsseln. Der Empfänger kann den Hash-Wert der empfangenen Nachricht berechnen und ihn mit der entschlüsselten Signatur vergleichen, um sicherzustellen, dass die Daten nicht manipuliert wurden.

- Public-Key-Infrastruktur (PKI): PKI ist ein System, das die Verwaltung von öffentlichen Schlüsseln in einer sicheren Umgebung ermöglicht. Es besteht aus Zertifizierungsstellen, die digitale Zertifikate ausstellen, die die Echtheit der öffentlichen Schlüssel bestätigen. PKI spielt eine wichtige Rolle bei der Sicherstellung der Sicherheit von Kommunikation und Transaktionen im Internet, indem es die Identifizierung und den sicheren Austausch von Schlüsseln erleichtert. Siehe hierzu: Lernzusammenfassung LZ_013_PKI

- Anwendungen der Verschlüsselung: Verschlüsselung wird in verschiedenen Bereichen eingesetzt, um die Sicherheit von Daten zu gewährleisten. Dazu gehören die sichere Kommunikation über das Internet (z. B. verschlüsselte E-Mails, SSL/TLS für verschlüsselte Webseiten), der Schutz von persönlichen Informationen in Datenbanken und in der Cloud, die Sicherung von gespeicherten Daten auf mobilen Geräten und die Verschlüsselung von Dateien oder Festplatten.

Datenschutzgesetze und Compliance

- Schutz der personenbezogenen Daten
  Datenschutzgesetze haben das Hauptziel, personenbezogene Daten zu schützen. Dazu gehören Informationen, die eine identifizierte oder identifizierbare natürliche Person betreffen, wie Namen, Adressen, Geburtsdaten, Kontonummern, IP-Adressen und vieles mehr.
- Einwilligung und Transparenz
  Die meisten Datenschutzgesetze verlangen von Organisationen, dass sie die ausdrückliche Einwilligung der betroffenen Personen einholen, bevor sie deren personenbezogene Daten sammeln, verarbeiten oder teilen. Es ist auch erforderlich, transparente Informationen über den Zweck der Datenerhebung und -verarbeitung bereitzustellen.
- Datensparsamkeit und Zweckbindung
  Datenschutzgesetze legen oft fest, dass Unternehmen nur die für einen bestimmten Zweck erforderlichen Daten erheben und verwenden dürfen. Die Verwendung von Daten für andere Zwecke als den ursprünglich angegebenen ist normalerweise nur mit erneuter Einwilligung oder in spezifischen gesetzlich vorgesehenen Ausnahmefällen erlaubt.
- Rechte der Betroffenen
  Datenschutzgesetze gewähren den betroffenen Personen verschiedene Rechte, wie das Recht auf Auskunft über ihre gespeicherten Daten, das Recht auf Berichtigung ungenauer Daten, das Recht auf Löschung oder das Recht, der Verarbeitung ihrer Daten zu widersprechen.
- Datensicherheit
  Datenschutzgesetze verpflichten Organisationen dazu, angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit personenbezogener Daten zu gewährleisten und sie vor Verlust, Missbrauch oder unbefugtem Zugriff zu schützen.

Aufbewahrungsfristen: Quelle https://www.ihk.de/hamburg/produktmarken/beratung-service/recht-und-steuern/steuerrecht/abgabenrecht/aufbewahrungsfristen-geschaeftsunterlagen-1157174

Disaster Recovery

Disaster Recovery (DR) oder auch Notfallwiederherstellung bezeichnet die Strategien und Maßnahmen, die Unternehmen und Organisationen ergreifen, um ihre IT-Infrastruktur und Daten nach einem schweren Ausfall, einer Naturkatastrophe, einem Cyberangriff oder anderen unvorhergesehenen Ereignissen wiederherzustellen und den Geschäftsbetrieb möglichst schnell und effizient fortzusetzen. Das Hauptziel von Disaster Recovery ist es, den Schaden zu minimieren und Ausfallzeiten zu reduzieren, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Hier sind einige wichtige Aspekte des Disaster Recovery und Beispiele für DR-Maßnahmen:

- Risikoanalyse
  Eine umfassende Risikoanalyse ist der erste Schritt im Disaster Recovery-Prozess. Hierbei werden potenzielle Bedrohungen, Schwachstellen und Risiken identifiziert, die die IT-Infrastruktur und Daten gefährden könnten. Dazu gehören Naturkatastrophen wie Erdbeben, Überschwemmungen oder Stürme, aber auch menschliche Fehler, Hardwareausfälle, Cyberangriffe oder andere Bedrohungen.
- Backup-Strategien
  Eine effektive Disaster-Recovery-Strategie beinhaltet regelmäßige Backups von geschäftskritischen Daten und Systemen. Unternehmen sollten mehrere Kopien ihrer Daten an verschiedenen Standorten speichern, um sicherzustellen, dass im Falle eines Ausfalls die Daten wiederhergestellt werden können.
- Widerherstellungsziele (RTO, RPO)

Beim Disaster Recovery werden oft zwei wichtige Metriken berücksichtigt - das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO). Das RTO definiert die maximale akzeptable Ausfallzeit, d.h., wie lange es dauern darf, um den Betrieb nach einem Ausfall wieder aufzunehmen. Das RPO definiert den maximal akzeptablen Datenverlust, d.h., wie viel Datenverlust das Unternehmen im schlimmsten Fall tolerieren kann.

- Notfallpläne
  Unternehmen müssen detaillierte Notfallpläne erstellen, die klare Anweisungen enthalten, wie bei einem Ausfall vorgegangen werden soll. Diese Pläne sollten Rollen und Verantwortlichkeiten von Mitarbeitern, Kontaktinformationen, Vorgehensweisen und Verfahren zur Wiederherstellung von Daten und Systemen enthalten.
- Redundanz und Ausfallsicherheit
  Redundanz und Ausfallsicherheit spielen eine entscheidende Rolle im Disaster Recovery. Unternehmen können redundante Systeme, Netzwerke und Speicherlösungen implementieren, um sicherzustellen, dass kritische Dienste weiterhin verfügbar sind, selbst wenn ein Teil der Infrastruktur ausfällt.

Überwachung und Tests

Die Überwachung und Tests sind wichtige Aspekte im Bereich der Datensicherung und des Disaster Recovery. Sie dienen dazu, die Integrität, Verfügbarkeit und Wirksamkeit der Datensicherungsmaßnahmen und Notfallwiederherstellungspläne zu gewährleisten. Durch regelmäßige Überwachung und Tests können Schwachstellen und Probleme rechtzeitig erkannt und behoben werden, um im Ernstfall einen reibungslosen Betrieb sicherzustellen.

- Überprüfung Backup-Logs
  Die Backup-Software sollte Protokolle über jede durchgeführte Sicherung erstellen. Die Überprüfung dieser Protokolle ermöglicht es, sicherzustellen, dass die Backups ordnungsgemäß durchgeführt wurden und es keine Fehler oder Warnungen gibt.
- Monitoring des Speicherplatzes
  Es ist wichtig, den verfügbaren Speicherplatz auf den Datensicherungsmedien, wie Festplatten oder Bändern, zu überwachen. Dadurch kann verhindert werden, dass die Datensicherung aufgrund von Speicherkapazitätsproblemen fehlschlägt.
- Alarme und Benachrichtigungen
  Es sollte ein Überwachungssystem eingerichtet werden, das Alarme und Benachrichtigungen bei auftretenden Problemen, Fehlern oder Ausfällen der Datensicherung verschickt. Dadurch können Administratoren schnell reagieren und das Problem beheben.
- Tests der Wiederherstellungsfähigkeit
  - Backup-Wiederherstellungstests
    Es sollten regelmäßige Tests der Wiederherstellung durchgeführt werden, um sicherzustellen, dass die gesicherten Daten tatsächlich wiederhergestellt werden können. Dabei werden einzelne Dateien oder ganze Systeme aus den Backups wiederhergestellt und überprüft, ob sie ordnungsgemäß funktionieren.
  - Disaster-Recovery-Tests
    Disaster-Recovery-Tests simulieren einen kompletten Ausfall der IT-Infrastruktur und prüfen, ob die Notfallwiederherstellungspläne effektiv funktionieren. Dabei wird das Wiederherstellen des gesamten Systems und des Betriebs geübt.
  - Drills und Übungen
    Regelmäßige Drills und Übungen mit den Mitarbeitern können dazu beitragen, dass alle Beteiligten mit den Notfallwiederherstellungsplänen vertraut sind und wissen, wie sie im Ernstfall handeln müssen.

- Bewerten und aktualisieren
    - Regelmäßige Bewertung der Datensicherungsstrategien und -maßnahmen, um sicherzustellen, dass sie den aktuellen Geschäftsanforderungen entsprechen.
- Aktualisierung der Notfallpläne
    - Aktualisierung der Notfallwiederherstellungspläne und -prozesse, um Änderungen in der IT-Infrastruktur oder Geschäftsprozessen zu berücksichtigen.

Die Überwachung und Tests sind entscheidend, um sicherzustellen, dass die Datensicherung und das Disaster Recovery optimal funktionieren und dass Unternehmen im Falle eines Ausfalls oder einer Katastrophe schnell wieder in den Normalbetrieb übergehen können.