



## Inhalt:

- *Einführung*
- *Integrität*
- *Rechte*
- *Backup*



## Inhalt:

- *Einführung*
- *Integrität*
- *Rechte*
- *Backup*

- *Schäden*
- *Gesetze*
- *Grundprinzipien der Sicherheit*



*Die meisten Informationen werden mit IT erstellt, gespeichert, transportiert oder weiterverarbeitet. Informationen besitzen einen wesentlichen Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden.*

*Moderne Geschäftsprozesse sind ohne IT-Unterstützung nicht mehr vorstellbar. Eine zuverlässige Informationsverarbeitung ist für die Aufrechterhaltung des Betriebes unerlässlich.*

*Informationssicherheit ist nicht nur eine Frage der Technik, sondern auch stark von den organisatorischen und personellen Rahmenbedingungen abhängig.*

*Unter der Datensicherheit versteht man alle technischen und organisatorischen Maßnahmen zum Schutz der Daten vor Verfälschung, Zerstörung und unzulässiger Weitergabe.*



*Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig das IT-Grundschutzhandbuch (ab 2005 – IT-Grundschutz-Kataloge) unter [www.bsi.bund.de](http://www.bsi.bund.de).*

*Dieses Buch enthält Sicherheitsmaßnahmen für typische IT-Systeme und Hinweise für deren Umsetzung.*

*Jeder Administrator sollte mit diesem Buch vertraut sein.*



*Mängel im Bereich der Informationssicherheit können zu erheblichen Problemen führen. Die potentiellen Schäden lassen sich verschiedenen Kategorien zuordnen.*

- *Verlust der Verfügbarkeit:  
Wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Läuft ein IT-System nicht, können beispielsweise keine Geldtransaktionen, Online-Bestellungen durchgeführt werden oder andere Produktionsprozesse sind unmöglich. Aber auch wenn die Verfügbarkeit von bestimmten Informationen nur eingeschränkt ist, kann es zu Arbeitsbeeinträchtigungen in den Prozessen einer Firma oder Behörde kommen.*



- *Verlust der Vertraulichkeit:*  
*Man muss mit den personenbezogenen Daten eines Bürgers vertraulich umgehen. Interne Daten eines Unternehmens über Umsatz, Marketing, Forschung und Entwicklung interessieren die Konkurrenz. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.*
- *Verlust der Integrität:*  
*Gefälschte Daten können zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen.*
- *Verlust der Authentizität:*  
*Daten werden einer falschen Person zugeordnet. Zahlungsanweisungen oder Bestellungen können zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden.*



*Datenschutz und Datensicherheit werden im Wesentlichen durch folgende Gesetze geregelt:*

- *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung – BDSG, 1990, Neufassung 2003, zuletzt geändert 2009;*
- *Telekommunikationsgesetz – TKG, 2004;*
- *Telemediengesetz – TMG, 2007;*
- *Signaturgesetz – Gesetz über Rahmenbedingungen für elektronische Signaturen, 2001;*
- *diverse Landesdatenschutzgesetze.*



*Es gelten folgende Grundprinzipien der Sicherheit für ein IT-System:*

- *Authentifizierung;*
- *Autorisierung;*
- *Protokollierung.*





*Laut dem Prinzip der Authentifizierung müssen die Subjekte (Benutzer, Rechner oder Dienste) ein Konto innerhalb des Systems besitzen.*

*Das Konto enthält Anmeldename, Kennwort und weitere Charakteristiken.*

*Bevor ein Subjekt Zugriff auf die Ressourcen eines Systems erhält, muss es sich im System mit einem gültigen Anmeldennamen und einem dazu passenden Kennwort anmelden.*

*Die modernen Datenbanken bieten weitere AnmelDEMöglichkeiten an, z.B. kann die Datenbank das Betriebssystem mit der Überprüfung der Anmeldedaten beauftragen. Anmeldung mit Zertifikaten ist ebenfalls möglich.*



Laut dem Prinzip der Autorisierung muss ein System Zugriffsrechte implementieren.

Jeder Zugriff eines Benutzers auf eine Ressource im System soll dabei gemäß den klar differenzierten Zugriffsarten und Berechtigungen stattfinden.

Die Leserechte erlauben dabei eine Benutzung der Ressourcen, ohne sie zu ändern.

Die Änderungsrechte inkludieren normalerweise die Leserechte und bieten die Möglichkeit, die Ressourcen zu verändern.

Ein Benutzer, der die vollen Rechte auf eine Ressource besitzt, darf zusätzlich zu Änderungsrechten die Rechte an andere Subjekte übertragen.

Absolut notwendig ist auch die Verweigerung oder Entziehung der Rechte, die den Zugriff auf die Ressourcen gänzlich verbietet.



Laut dem Prinzip der Protokollierung müssen alle wichtigen Vorgänge vom System überwacht und protokolliert werden. Dazu gehören folgende Aktivitäten:

- Lesen, Verändern und Löschen von Daten;
- Recht, sich an der Datenbank anzumelden;
- Start, Mounten, Öffnen und Beenden der Datenbank;
- Benutzer- oder Gruppenkontenverwaltung (Rollen, Profile).

In den Protokollen müssen mindestens drei Angaben zu jedem Vorgang festgehalten sein: wer (welches Konto), was (Aktion) und wann (Datum und Uhrzeit) gemacht hat.

Oracle bezeichnet Protokollierung als Auditing. Oracle bietet umfangreiche Mechanismen an, um Auditing flexibel und ausführlich zu organisieren. Das sind Rechte (Privilegien), spezielle Tabellen, Dateien.



*Die konsequente Durchführung der genannten drei Prinzipien gewährleistet ein sicheres IT-System.*

*Leider ist die optimale Durchsetzung nur selten möglich, weil dem andere Faktoren entgegenwirken.*

*Beispiel:*

*Ein Web-Server stellt normalerweise seine Dienste für alle Benutzer zur Verfügung. Man kann nicht jeden Benutzer in der Welt identifizieren und für ihn ein eigenes Konto pflegen. Der Web-Server ordnet die Anfragen aller Benutzer einem besonderen (pauschalen) Konto zu und beantwortet sie anschließend. Mit diesem Konto wird es an der Datenbank angemeldet. Damit liegt hier aber schon eine Verletzung des ersten Prinzips (Authentifizierung) vor. Dies erlaubt einem potenziellen Angreifer, unzählige und unsinnige Anfragen an den Web-Server (und weiter an die Datenbank) zu schicken. Es ist in entscheidendem Maße vom Programmcode der Anwendungen abhängig, wie es darauf reagiert wird.*



## Inhalt:

- *Einführung*
- *Integrität*
- *Rechte*
- *Backup*



## Definition

*Integrität (Konsistenz) der Datenbank ist ein Zustand der Daten, in dem sie korrekt, vollständig und widerspruchsfrei sind.*

*Folgende Arten der Integrität werden unterscheiden:*

- Semantische Integrität – Werte des Attributes gehören zu einem Wertebereich, richtige Datentypen sind für die Attribute ausgewählt, keine Tippfehler.*
- Referentielle Integrität – Korrektheit der Primär- und Fremdschlüssel, Existenz der Verweise zwischen den Tabellen.*
- Logische Integrität – Transaktionen, die zusammengehörenden Operationen.*



*Zwei Wege, die Integrität zu gewährleisten:*

- *Ebene der Datenbank (bessere Lösung).*
- *Ebene der Anwendung (zusätzliche Lösung).*

*Alle modernen Datenbanken stellen die Mittel zur Verfügung, um die Integrität der Daten zu wahren. Das sind normalerweise die Klauseln in den DDL-Anweisungen.*

*Die Überwachung der Integrität durch die Anwendung sollte als zusätzliche Methode betrachtet werden.*



## *Vorteile der Definition der Integritätsbedingungen auf der Datenbank-Ebene:*

- *Datenbank selbst gewährleistet die Konsistenz des Datenbestandes, somit sind die inkonsistenten Zustände der gespeicherten Daten unmöglich.*
- *Integritätsüberprüfung kann ein- oder ausgeschaltet werden, z.B. zwecks Leistungserhöhung beim Import.*
- *Datenbank liefert mehrere standardisierte Möglichkeiten für die Integritätsbedingungen.*
- *Die Integrität der Datenbank ist von einzelnen Anwendungen unabhängig. Definierte Bedingungen gelten für alle Anwendungen.*
- *Schnellere Entwicklung der Anwendungen, da Integrität nicht jedes mal implementiert werden soll.*





*DML-Operationen, die zur Verletzung der Integrität führen können:*

- *Neue Datensätze einfügen (INSERT).*
- *Vorhandene Datensätze korrigieren (UPDATE).*
- *Vorhandene Datensätze löschen (DELETE).*

*DDL-Operationen (ALTER, DROP, RENAME) können ebenfalls u.U. Verlust der Integrität als Folge haben.*

*Die Zugriffskontrolle wird hier nicht betrachtet.*



*Folgende (disjunktive) Aktionen sind möglich, falls die Integrität während einer Operation verletzt wird:*

- Abbrechen der Operation und Zurücksetzen der Datenbank auf den Zustand vor der Operation (rollback).*
- Propagieren der Operation auf alle beteiligten Tabellen (cascade).*
- Die betroffenen Attribute auf Null-Wert setzen (set null).*



*Referenzielle Integrität: Die Werte eines Fremdschlüssels müssen auch als Werte des Primärschlüssels vorhanden sein.*

<u>Name</u>	Anzahl MA
Maxi-Taxi	300
Luxi-Taxi	20
Fixi-Taxi	90

<u>Name</u>	<u>KFZ</u>	Modell	Baujahr
Maxi-Taxi	BAZ-0815	VW	2011
Luxi-Taxi	BBQ-2322	Mercedes	2013
Luxi-Taxi	BZA-3159	BMW	2011
Maxi-Taxi	BKA-1122	Mercedes	2013
Fixi-Taxi	BSR-4253	Skoda	2017



## Typen von Constraints:

- *PRIMARY KEY – Attribut (oder Kombination der Attribute) bildet primären Schlüssel. Automatisch wird immer ein Index angelegt (Oracle).*
- *FOREIGN KEY – Attribut (oder Kombination der Attribute) bildet primären Schlüssel in einer anderen Tabelle.*
- *ON DELETE CASCADE (Teil von FOREIGN KEY) – Löschen eines Datensatzes in der Tabelle mit PK verursacht das Löschen der Datensätze in der Tabelle mit FK, wo dieses Constraint steht.*
- *NOT NULL – Attribut muss einen Wert haben.*
- *UNIQUE – Werte eines Attributs (oder einer Kombination der Attribute) sind einmalig.*
- *CHECK – Logischer Ausdruck ist wahr.*



## Beispiele:

```
CREATE TABLE Studenten
```

```
(
```

```
  MatrNr INTEGER PRIMARY KEY,
```

```
  Name   VARCHAR(30) NOT NULL,
```

```
  Semester INTEGER CHECK Semester BETWEEN 1 AND 13
```

```
);
```

```
CREATE TABLE Professoren
```

```
(
```

```
  PersNr INTEGER PRIMARY KEY,
```

```
  Name   VARCHAR(30) NOT NULL,
```

```
  Rang   CHAR(2) CHECK (Rang IN ('C2', 'C3', 'C4')),
```

```
  Raum   INTEGER UNIQUE
```

```
);
```



## Beispiele:

```
CREATE TABLE voraussetzen
```

```
(
```

```
  Vorgaenger INTEGER REFERENCES Vorlesungen(VorLNr)
```

```
  ON DELETE CASCADE,
```

```
  Nachfolger INTEGER REFERENCES Vorlesungen(VorLNr)
```

```
  ON DELETE NO ACTION,
```

```
  PRIMARY KEY (Vorgaenger, Nachfolger)
```

```
);
```

```
CREATE TABLE pruefen
```

```
(
```

```
  MatrNr INTEGER REFERENCES Studenten ON DELETE CASCADE,
```

```
  VorLNr INTEGER REFERENCES Vorlesungen,
```

```
  PersNr INTEGER REFERENCES Professoren,
```

```
  Note NUMERIC(2,1) CHECK (Note BETWEEN 0.7 AND 5.0),
```

```
  PRIMARY KEY (MatrNr, VorLNr)
```

```
);
```



*Zusätzlich zu Constraints bieten viele Datenbanken noch Trigger zu Wahrung der Konsistenz an. Unter einem Trigger versteht man eine Prozedur oder eine Funktion, die nur bei bestimmten Ereignissen automatisch gestartet wird. Das sind nämlich Ereignisse (Operationen), bei denen die Integrität der Datenbank verletzt werden kann.*

*Folgende Auslöser der Trigger existieren:*

- DML-Operatoren INSERT, DELETE, UPDATE.*
- DDL-Operatoren CREATE, ALTER, DROP.*
- An- und Abmeldung eines Benutzers, Start/Stop der Datenbank.*

*Man kann manchmal den Start des Triggers konkretisieren:*

- BEFORE – vor der Änderung.*
- AFTER – nach der Änderung.*
- INSTEAD OF – statt der Änderung.*



## Inhalt:

- *Einführung*
- *Integrität*
- *Rechte*
- *Backup*





*Verschiedene Datenbanken liefern unterschiedliche Konzepte für Zugriffsrechte auf die Daten. Weiter wird eine Anlehnung an Oracle-Datenbank betrachtet.*

*Zentrale Stelle im Oracle-Konzept nimmt der Begriff User (Benutzer), auch Schema benannt. Die Anwender oder die Anwendungen melden sich bei der Datenbank als ein bestimmter Benutzer an. Da wird ein bestimmtes ERM implementiert, das für die Anwendung entwickelt wurde. Die Benutzer haben nicht unbedingt freien Zugriff auf Tabellen von einander, aber entsprechende Rechte können durchaus erteilt werden.*

*Somit besteht eine Oracle-Datenbank aus unterschiedlichen Schemen (User), innerhalb von denen ERM realisiert sind. Es gibt vordefinierte Benutzer SYS und SYSTEM, die sämtliche Rechte standardmäßig haben. Alle anderen Benutzer müssen erstellt und mit Zugriffsrechten versehen werden.*



*Es ist empfehlenswert, klare Richtlinien in einem Unternehmen zu erarbeiten, die den Zugriff auf die Datenbank festlegen:*

- *wer darf zugreifen;*
- *auf welche Ressourcen (Tabellen, Spalten, View) darf zugegriffen werden;*
- *welche Zugriffsart (z.B. "Lesen", "Ändern", "Index erstellen");*
- *an welchen Tagen und zu welchen Uhrzeiten;*
- *von welchen Computern aus;*
- *wer erlaubt den Zugriff;*
- *wer muss informiert werden;*
- *wie wird der Zugriff protokolliert;*
- *wie wird der Zugriff abgerechnet.*



*Datenbank implementiert folgende Sicherheitsmechanismen:*

- *Discretionary Access Control (DAC). Regeln für Zugriffe auf Objekte werden festgelegt. Ein Benutzer kann auf Objekte zugreifen, nur wenn er entsprechende Rechte hat. Eine Regel in DAC sieht so aus:*  
$$\{ O, S, R, P, F \}$$
  - *O ist Menge von Objekten (Tabellen, Indizes, ...);*
  - *S ist Menge von Subjekten (Benutzer, Prozesse, ...);*
  - *R ist Menge von Zugriffsrechten (Lesen, Schreiben, ...);*
  - *P ist Prädikat, das über Zugriff entscheidet;*
  - *F ist ein Recht, die Rechte zu vergeben.*
- *Mandatory Access Control (MAC). Hierarchie der Prozesse wird festgelegt. Jeder Prozess bekommt eine Markierung mit einem bestimmten Niveau (Einstufung). Prozesse können mit einander nur dann kommunizieren (Daten austauschen), wenn ihre Markierungen vom gleichen Niveau sind. Benutzer können nur dann die Objekte sehen, wenn sie einen MAC-Zugriff haben.*



*Datenbank bietet den Benutzern folgende DAC-Rechte (Privilegien) an:*

- *Systemprivilegien berechtigen zu Systemoperationen wie*
  - *Anmeldung;*
  - *Anlegen, Löschen von Tabellen, Ändern der Struktur der Tabellen;*
  - *Anlegen, Löschen von Benutzern;*
  - *Anlegen, Löschen von Prozeduren/Funktionen;*
  - *Abfragen von Systemtabellen;*
  - *Verwaltung von Tablespaces; u.ä.*
- *Objektprivilegien berechtigen zu Objektoperationen wie*
  - *Abfragen der Tabellen;*
  - *Ändern der Inhalte der Tabellen;*
  - *Verwenden von Funktionen in Abfragen; u.ä.*

*Es ist empfehlenswert, eine sinnvolle Rollenmatrix mit Privilegien zu erstellen. Die einzelnen Benutzer bekommen dabei keine Privilegien direkt zugewiesen, sondern die Rollen werden den Benutzern zugewiesen.*



## Beispiel:

```
DROP USER Student07;
```

```
CREATE USER Student07 IDENTIFIED BY system  
  DEFAULT TABLESPACE users  
  TEMPORARY TABLESPACE temp  
  QUOTA UNLIMITED ON users;
```

So ein erstellter Benutzer muss nach der ersten Anmeldung sofort sein Password ändern, z.B. so:

```
ALTER USER Student07 IDENTIFIED BY System01;
```



*Es gibt eigentlich nur zwei Befehle für Rechteverwaltung:*

- *GRANT – Rechte dem Benutzer vergeben.*
- *REVOKE – Rechte dem Benutzer entziehen.*

*Es ist aber nicht empfehlenswert, die Rechte einem einzelnen Benutzer zu vergeben. Stattdessen werden die Benutzergruppen (Rollen) erstellt, und die einzelnen Benutzer werden den Rollen zugeordnet. Die Zugriffsrechte sind den Rollen zu erteilen.*

```
DROP ROLE StudentRole;
```

```
CREATE ROLE StudentRole;
```

```
GRANT CREATE session, CREATE table, CREATE view,  
      CREATE synonym, CREATE procedure, CREATE trigger  
TO StudentRole;
```

```
GRANT StudentRole TO Student07;
```



*Beispiele (wie erwähnt, nicht unbedingt empfehlenswert):*

```
GRANT SELECT ON Tabelle13 TO Student07, Student08;
```

```
GRANT INSERT, SELECT ON Student03.TabelleA TO Student07;
```

```
GRANT ALL ON database TO dba_user02;
```

*Man kann Rechte auf einzelne Spalten vergeben:*

```
GRANT UPDATE (Spalte1), INSERT (Spalte2, Spalte3)  
ON Tabelle52 TO Student07;
```



## Inhalt:

- Einführung
- Integrität
- Rechte
- Backup

- 
- A light blue callout box with a black border and rounded corners. It has a long, thin tail pointing towards the 'Backup' item in the left list. Inside the box is a list of six items.
- Definition
  - Beispiele
  - Medien
  - Methoden
  - Arten
  - Strategien





Definition: Backup, oder Datensicherung, ist eine Speicherung der Daten, mit der ein System oder dessen Komponenten nicht direkt arbeiten.

*Eigenschaften:*

- *Ein Backup kann mehrere Dateien und Verzeichnisse beinhalten.*
- *Ein Backup kann wie eine Datei oder mehrere Dateien und Verzeichnisse aussehen.*
- *Ein Backup kann verschlüsselt und/oder komprimiert sein.*
- *Ein Backup kann sich auf einem Datenträger befinden, oder sich über mehrere Datenträger verbreiten.*

Definition: Backup-Archiv (oder einfach Archiv) ist eine Sammlung von mehreren Backups.



*Ein Backup wird mit unterschiedlichen Absichten erstellt:*

- *Wiederherstellung der Daten im Falle eines Absturzes.*
- *Wiederherstellung des Zustandes eines Systems zu einem bestimmten Zeitpunkt für statistische Zwecke (z.B. Jahresbericht einer Versicherung).*
- *Wiederherstellung des Zustandes eines Systems zu einem bestimmten Zeitpunkt für planmäßige Funktionalität einer Anwendung (z.B. Forschungsprojekte, Architektur).*

*Regel:* *In allen nicht privaten Anwendungen und Systemen muss man immer Backup planen und regelmäßig durchführen.*

*Aufbewahrung und Vernichtung des Backups regeln die firmen-internen Richtlinien und die gesetzlichen Vorgaben.*



*Ein Backup darf man nicht mit den RAID-Lösungen (Redundant Array of Inexpensive/Independent Disks) verwechseln.*

*Ein RAID-System speichert die Informationen mehrfach (redundant) auf den Festplatten. Stürzt eine Festplatte ab, so können die Daten im laufenden Betrieb von einer anderen gelesen oder auf eine andere geschrieben werden. Dieses System gewährleistet einen ununterbrochenen Betrieb auch beim Ausfall eines Datenträgers. Die kaputte Festplatte kann im laufenden Betrieb ausgewechselt werden, und das RAID-System wird den Datenbestand automatisch nach und nach abgleichen.*

*Fast alle Betriebssysteme unterstützen RAID softwaremäßig.*

*Die hardwaremäßigen RAID-Systeme sind von dem Betriebssystem unabhängig, so dass das Betriebssystem ein RAID nicht mal sieht.*

*Ein RAID-System erfüllt keine Funktionen von Backup.*

*Ein RAID-System kann als Speicherort für Backup verwendet werden.*



## RAID

Unter **RAID** (Redundant Array of Inexpensive/Independent Disks) sind verschiedene Fehlertoleranz-Lösungen bekannt. Im Allgemeinen geht es darum, dass mehrere (kleinere) Festplatten in zweierlei Hinsichten flexibler als eine (große) verwendet werden können.

**RAID 0 – Striping ohne Parität**, eigentlich keine Fehlertoleranz

- Mindestens zwei Festplatten müssen vorhanden sein.
- Alle Informationen werden in Blöcken stückweise parallel auf mehrere Festplatten geschrieben.
- Durch Parallelität wird eine sehr hohe Performance bei den Datenträgerzugriffen erzielt.
- Der Ausfall einer Festplatte hat den totalen Datenverlust zur Folge.

### RAID 1 – Spiegelung oder Duplizierung

- Mindestens zwei Festplatten müssen vorhanden sein.
- Daten werden doppelt abgelegt, jeweils ein Datensatz auf jeder Festplatte.
- Die Performance gleicht der bei Verwendung einer Festplatte.
- Bei Ausfall einer Festplatte sind alle Informationen auf der anderen Festplatte sofort benutzbar.
- Bei laufendem Betrieb kann die ausgefallene Festplatte gewechselt werden.

### RAID 5 – Striping mit Parität

- Mindestens drei Festplatten müssen vorhanden sein.
- Alle zu speichernden Informationen werden in Blöcke geteilt und parallel auf die Festplatten geschrieben.
- Zusätzlich wird die Prüfsumme von den Blöcken ermittelt und auch über mehrere Festplatten verteilt.
- Es wird eine sehr hohe Performance bei den Datenträgerzugriffen erzielt, allerdings etwas niedriger als bei RAID 0.
- Bei Ausfall einer Festplatte können alle Daten dank der Paritätsinformationen nach einem mathematischen Verfahren automatisch und im laufenden Betrieb wiederhergestellt werden.

Die Windows-Professional-Versionen bieten nur den RAID-Level 0 an, die Server-Versionen unterstützen außerdem RAID-Level 1 und 5. Mehrere Festplatten erscheinen für den Benutzer als ein einziger Datenträger, dem nur ein Buchstabe zugewiesen ist (beispielsweise F:).



## RAID

Unter **RAID** (Redundant Array of Inexpensive/Independent Disks) sind verschiedene Fehlertoleranz-Lösungen bekannt. Im Allgemeinen geht es darum, dass mehrere (kleinere) Festplatten in zweierlei Hinsichten flexibler als eine (große) verwendet werden können.

**RAID 0 – Striping ohne Parität**, eigentlich keine Fehlertoleranz

- Mindestens zwei Festplatten müssen vorhanden sein.
- Alle Informationen werden in Blöcken stückweise parallel auf mehrere Festplatten geschrieben.
- Durch Parallelität wird eine sehr hohe Performance bei den Datenträgerzugriffen erzielt.
- Der Ausfall einer Festplatte hat den totalen Datenverlust zur Folge.

## RAID 1 – Spiegelung oder Duplizierung

- Mindestens zwei Festplatten müssen vorhanden sein.
- Daten werden doppelt abgelegt, jeweils ein Datensatz auf jeder Festplatte.
- Die Performance gleicht der bei Verwendung einer Festplatte.
- Bei Ausfall einer Festplatte sind alle Informationen auf der anderen Festplatte sofort benutzbar.
- Bei laufendem Betrieb kann die ausgefallene Festplatte gewechselt werden.

Parität  
platten müssen vorhanden

Informationen werden in  
allel auf die Festplatten

ifsumme von den Blöcken er-  
mehrere Festplatten verteilt.  
e Performance bei den  
erzielt, allerdings etwas  
0.

platte können alle Daten

dank der Paritätsinformationen nach einem  
mathematischen Verfahren automatisch und im  
laufenden Betrieb wiederhergestellt werden.

Die Windows-Professional-Versionen bieten nur den  
RAID-Level 0 an, die Server-Versionen unterstützen  
außerdem RAID-Level 1 und 5.

Mehrere Festplatten erscheinen für den Benutzer  
als ein einziger Datenträger, dem nur ein Buchstabe  
zugewiesen ist (beispielsweise F:).



## RAID

Unter **RAID** (Redundant Array of Inexpensive/Independent Disks) sind verschiedene Fehlertoleranz-Lösungen bekannt. Im Allgemeinen geht es darum, dass mehrere (kleinere) Festplatten in zweierlei Hinsichten flexibler als eine (große) verwendet werden können.

**RAID 0 – Striping ohne Parität**, eigentlich keine Fehlertoleranz

- Mindestens zwei Festplatten müssen vorhanden sein.
- Alle Informationen werden in Blöcken stückweise parallel auf mehrere Festplatten geschrieben.
- Durch Parallelität wird eine sehr hohe Performance bei den Datenträgerzugriffen erzielt.
- Der Ausfall einer Festplatte hat den totalen Datenverlust zur Folge.

## RAID 1 – Spiegelung oder Duplizierung

- Mindestens zwei Festplatten müssen vorhanden sein.
- Daten werden doppelt abgelegt, jeweils ein Datensatz auf jeder Festplatte.
- Die Performance gleicht der bei Verwendung einer Festplatte.
- Bei Ausfall einer Festplatte sind alle Informationen auf der anderen Festplatte sofort benutzbar.
- Bei laufendem Betrieb kann die ausgefallene Festplatte gewechselt werden.

## RAID 5 – Striping mit Parität

- Mindestens drei Festplatten müssen vorhanden sein.
- Alle zu speichernden Informationen werden in Blöcke geteilt und parallel auf die Festplatten geschrieben.
- Zusätzlich wird die Prüfsumme von den Blöcken ermittelt und auch über mehrere Festplatten verteilt.
- Es wird eine sehr hohe Performance bei den Datenträgerzugriffen erzielt, allerdings etwas niedriger als bei RAID 0.
- Bei Ausfall einer Festplatte können alle Daten dank der Paritätsinformationen nach einem mathematischen Verfahren automatisch und im laufenden Betrieb wiederhergestellt werden.

Die Windows-Professional-Versionen bieten nur den RAID-Level 0 an, die Server-Versionen unterstützen außerdem RAID-Level 1 und 5.

Mehrere Festplatten erscheinen für den Benutzer als ein einziger Datenträger, dem nur ein Buchstabe zugewiesen ist (beispielsweise F:).



*Jede Datenbank enthält eigene Software, die eine Datensicherung gewährleistet.*

*Oracle bietet mehrere Softwareprodukte an, die Backup und Wiederherstellung der Daten durchführen:*

- *exp/imp (ältere Versionen);*
- *expdp/impdp (neuere Versionen);*
- *RMAN (Recovery Manager).*

*Durch Verwendung von vielen Einstellungsparametern lassen sich alle Backup-Programme sehr flexibel einsetzen.*



Außerdem gibt es eine Vielzahl von Drittanbietern und On-Board-Mitteln des Betriebssystems, die ebenfalls maßgeschneiderte Lösungen für Backup liefern. Das sind:

- Befehle *cp*, *tar*, *bzip*, *gzip*, *dd* unter Linux/UNIX.
- Befehle *copy*, die Konsole Server-Sicherung unter MS Windows Server 2016.
- Acronis True Image 2014 für MS Windows und für Linux.
- Paragon Backup & Recovery 2014 für MS Windows.
- Fwbackups und Bacula für Linux.





## Medien für Backup:

- *Festplatte des lokalen Computers – DAS (Direct Attached Storage).*
- *Festplatte im Netzwerk – NAS (Network Attached Storage), SAN (Storage Area Network).*
- *Magnetband, Bandlaufwerk mit Roboter – bis zu 4 GiB.*
- *CD/DVD/Blu-Ray.*
- *USB-Geräte.*
- *FireWire-Geräte.*
- *Cloud im Internet, Sicherheit ist aber bedenklich.*

*Stehen wenige Exemplare der Medien zur Verfügung, deren Kapazitäten begrenzt sind, dann wird Generationsprinzip verwendet, z.B. Großvater–Vater–Sohn.*



*Bei diesem Verfahren Großvater–Vater–Sohn werden mehrere Datenträger verwendet, normalerweise ein Datenträger je Sicherung.*

*Stehen für die Sicherung drei Datenträger zur Verfügung, erfolgt die*

- erste Sicherung auf dem ersten Datenträger (Großvater);*
- zweite Sicherung auf dem zweiten Datenträger (Vater);*
- dritte Sicherung auf dem dritten Datenträger (Sohn);*
- vierte Sicherung wieder auf dem ersten Datenträger, dabei wird der Vater zum Großvater, der Sohn zum Vater und der Großvater zum Sohn.*

*Mit weiteren Backups wird dieses Prinzip systematisch fortgeführt. Der Vorteil liegt darin, dass die Datensicherungen schrittweise zurückverfolgt und die Datenträger effektiv ausgelastet werden können. Je mehr Datenträger verwendet werden, desto sicherer ist dieses Verfahren.*



Die Sicherungsmethoden beziehen sich auf die Betriebsart der Datenbank. Zwei Arten von Backup/Recovery existieren:

- Online Backup, Hot Backup. Die Datenbank darf nicht ausgeschaltet werden, und die Daten werden im laufenden Betrieb gesichert. Die Datenbank läuft in einem normalen Arbeitsmodus, d.h. die Daten können in den Tabellen verarbeitet werden. Zu gleicher Zeit laufen auch die Backup-Prozesse. Mehrere Prozesse können wirklich gleichzeitig laufen, was zu enormen Zeitersparnissen führt. Dabei gibt es Gefahr, dass sich der Datenbestand im Backup in einem nicht konsistenten Zustand befindet. Um es zu vermeiden, liefern die Datenbanken (z.B. ORACLE) ihre spezifischen Lösungen.
- Offline Backup, Cold Backup. Die Datenbank darf für eine bestimmte Zeit ausgeschaltet werden. Die Datenbank ist heruntergefahren, alle Dateien sind geschlossen. Die Backup-Prozesse kopieren eigentlich die geschlossenen Dateien. Der Datenbestand im Backup befindet sich immer in einem konsistenten Zustand.



Die Sicherungsarten beziehen sich auf den Umfang der zu speichernden Daten. In sehr vielen Fällen werden nicht alle Daten in einem Unternehmen täglich geändert, sondern relativ geringere Teile davon. Man unterscheidet folgende Sicherungsarten:

- Normale Sicherung. Alle dafür ausgewählten Daten werden in den Backup übertragen und auf der Festplatte als gesichert markiert. Werden einige Daten demnächst geändert, dann wird diese Markierung gelöscht. Somit weiß das Sicherungsprogramm beim nächsten Lauf, welche Daten wurden schon gesichert und welche nicht.
- Kopie-Sicherung. Sie funktioniert ähnlich wie eine normale Sicherung, aber die Daten werden nicht als gesichert markiert.
- Tägliche Sicherung. Nur die heute geänderten Daten werden gesichert. Ebenfalls erfolgt die Markierung der gesicherten Daten.



- Inkrementelle Sicherung. Nicht alle ausgewählten Daten werden gesichert, sondern nur die geänderten. Die gesicherten Daten werden wiederum als gesichert markiert, somit werden sie beim nächsten Lauf des Sicherungsprogramms nicht mitgenommen (falls sie dazwischen nicht geändert wurden).

Eine inkrementelle Sicherung ist normalerweise viel kleiner als die normale Sicherung, und alle inkrementellen Sicherungen sind mehr oder weniger gleich groß.

Wiederherstellung – zuerst die letzte normale Sicherung und dann alle inkrementellen Sicherungen in richtiger Reihenfolge.

Vorteil – die inkrementellen Sicherungen nehmen weniger Zeit und Speicherplatz in Anspruch als differenzielle.

Nachteil – großer Aufwand bei Wiederherstellung.



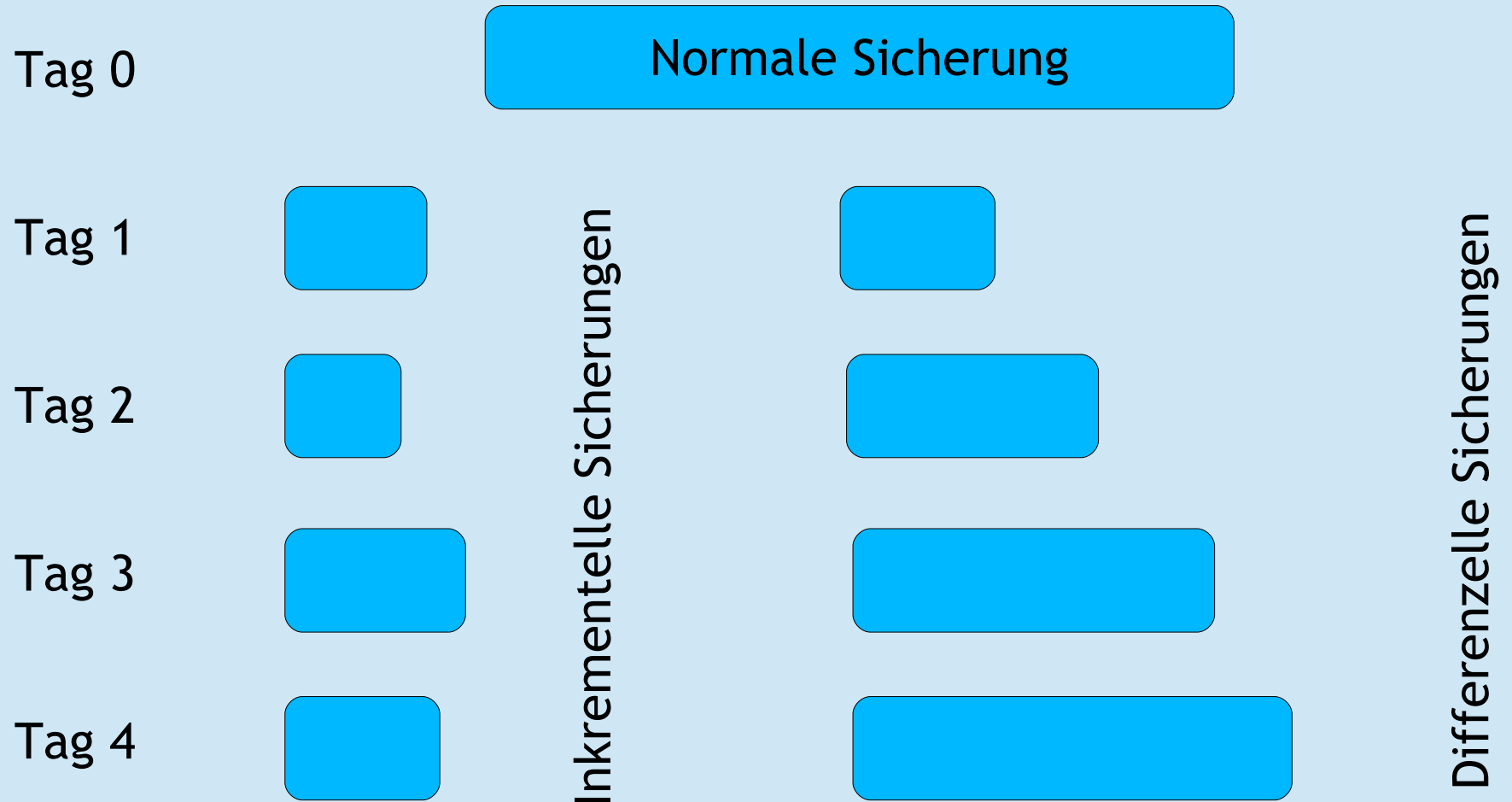
- Differenzielle Sicherung. Nicht alle ausgewählten Daten werden gesichert, sondern nur die geänderten. Die gesicherten Daten werden aber nicht als gesichert markiert, somit werden sie beim nächsten Lauf des Sicherungsprogramms wieder mitgenommen (auch wenn sie dazwischen nicht geändert wurden).

*Die Größe einer differenziellen Sicherung wächst von einem Lauf des Sicherungsprogramms zum nächsten.*

*Wiederherstellung – zuerst die letzte normale Sicherung und dann die letzte differenzielle Sicherung.*

*Vorteil – weniger Aufwand bei Wiederherstellung.*

*Nachteil – die differenziellen Sicherungen nehmen mehr Zeit und Speicherplatz in Anspruch in Vergleich zu inkrementellen.*





*Eine Sicherungsstrategie empfiehlt bestimmte Sicherungsarten in bestimmter Reihenfolge, damit die Wiederherstellung der Daten im Notfall geordnet ablaufen kann.*

*Offensichtlich sind folgende Strategien:*

- Regelmäßig nur die normalen Sicherungen, z.B. monatlich.*
- Normale Sicherung + inkrementelle Sicherungen, z.B. einmal im Jahr eine normale Sicherung und monatlich eine inkrementelle.*
- Normale Sicherung + differenzielle Sicherungen, z.B. einmal im Jahr eine normale Sicherung und monatlich eine differenzielle.*

*Wichtig:* *Anforderungen des Unternehmens und Speicherbedarf müssen berücksichtigt werden.*



