# Datensicherung und ihre Bedeutung für Datensicherheit und Datenschutz

## 1. Was ist Datensicherung?

Datensicherung bezeichnet den Prozess der Erstellung und Speicherung von Kopien wichtiger Daten, um deren Verlust durch Hardwarefehler, Cyberangriffe oder menschliche Fehler zu verhindern. Sie ist ein wesentlicher Bestandteil der Datensicherheit und trägt zur Erfüllung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bei. Zudem unterstützt eine effektive Datensicherung die Einhaltung datenschutzrechtlicher Vorgaben, indem sie den Schutz personenbezogener Daten sicherstellt.  
  
Quelle: Datenschutzexperte.de, „Datensicherung als Schlüsselfaktor des Datenschutzes“, abrufbar unter: [https://www.datenschutzexperte.de](https://www.datenschutzexperte.de/blog/datensicherung?utm\_source=chatgpt.com)

## 2. Gründe für Datensicherung

Die Notwendigkeit der Datensicherung ergibt sich aus verschiedenen Faktoren:  
- \*\*Schutz vor Datenverlust\*\*: Hardwaredefekte, Softwarefehler oder versehentliches Löschen können zu unwiederbringlichem Datenverlust führen.  
- \*\*Abwehr von Cyberangriffen\*\*: Schadsoftware wie Ransomware kann Daten verschlüsseln oder zerstören.  
- \*\*Sicherstellung der Betriebsfähigkeit\*\*: Unternehmen sind auf kontinuierlichen Datenzugriff angewiesen, um Geschäftsprozesse aufrechtzuerhalten.  
- \*\*Einhaltung gesetzlicher Vorschriften\*\*: Datenschutzgesetze wie die DSGVO verlangen die sichere Speicherung und Wiederherstellbarkeit von Daten.

## 3. Arten von Backups

- \*\*Voll-Backup\*\*: Erstellung einer vollständigen Kopie aller Daten. Vorteil: Einfache Wiederherstellung; Nachteil: Hoher Speicherbedarf.  
- \*\*Inkrementelles Backup\*\*: Sicherung nur der Daten, die seit dem letzten Backup verändert wurden. Vorteil: Spart Speicherplatz; Nachteil: Komplexere Wiederherstellung.  
- \*\*Differentielles Backup\*\*: Speicherung aller Änderungen seit dem letzten Voll-Backup. Vorteil: Schnellere Wiederherstellung als beim inkrementellen Backup; Nachteil: Erhöhter Speicherbedarf im Vergleich zum inkrementellen Backup.  
- \*\*Spiegel-Backup (Mirror Backup)\*\*: Erstellung einer 1:1-Kopie in Echtzeit, bei der alle Änderungen sofort synchronisiert werden.  
  
Quelle: Crossdelta.de, „Backup-Strategien im Unternehmen“, abrufbar unter: [https://www.crossdelta.de](https://www.crossdelta.de/blog/datensicherung-im-unternehmen-strategien-und-best-practices-2795/?utm\_source=chatgpt.com)

## 4. Backup-Strategien

Eine durchdachte Backup-Strategie ist unerlässlich:  
- \*\*3-2-1-Regel\*\*: Drei Kopien der Daten auf zwei verschiedenen Medien, eine Kopie extern gespeichert.  
- \*\*GFS-Strategie (Großvater-Vater-Sohn)\*\*: Strukturierte Sicherung mit täglichen, wöchentlichen und monatlichen Backups.  
- \*\*Cloud-Backups\*\*: Nutzung externer Anbieter zur Sicherung von Daten in der Cloud, wobei auf Verschlüsselung und Zugriffskontrollen geachtet werden muss.

## 5. Speicherorte für Backups

- \*\*Lokale Speichermedien\*\*: Externe Festplatten, NAS-Systeme oder Bandlaufwerke bieten schnellen Zugriff, sind jedoch anfällig für physische Schäden oder Diebstahl.  
- \*\*Netzwerkspeicher (NAS/SAN)\*\*: Sicherung innerhalb des Unternehmensnetzwerks mit redundanten Speicherlösungen.  
- \*\*Cloud-Speicher\*\*: Externe Anbieter bieten skalierbare Backup-Lösungen mit automatischer Synchronisation.  
- \*\*Offline-Backups\*\*: Trennung von Backup-Systemen vom Netzwerk zum Schutz vor Cyberangriffen.  
  
\*\*Praxisbeispiele:\*\*  
- \*\*Erfolgreiche Datensicherung\*\*: Ein mittelständisches Unternehmen wurde Opfer eines Ransomware-Angriffs. Dank regelmäßiger Backups auf externen Speichermedien konnte der Betrieb schnell wiederhergestellt werden, ohne Lösegeld zu zahlen. ([Crossdelta.de](https://www.crossdelta.de))  
- \*\*Fehlende Datensicherung\*\*: Ein anderes Unternehmen erlitt durch einen Cyberangriff einen massiven Datenverlust. Aufgrund fehlender oder veralteter Backups gingen wichtige Geschäftsdaten unwiederbringlich verloren. ([Crossdelta.de](https://www.crossdelta.de))

## 6. Wichtige Aspekte der Datensicherung

- \*\*Automatisierung\*\*: Regelmäßige, automatische Sicherungen minimieren menschliche Fehler.  
- \*\*Verschlüsselung\*\*: Schutz vor unbefugtem Zugriff durch Verschlüsselung der Backup-Dateien.  
- \*\*Redundanz\*\*: Mehrere Sicherungskopien verhindern Datenverluste durch defekte Speichermedien.  
- \*\*Regelmäßige Tests\*\*: Überprüfung der Wiederherstellbarkeit, um sicherzustellen, dass Backups im Ernstfall nutzbar sind.

## 7. Wiederherstellung von Daten

- \*\*Disaster Recovery\*\*: Planung und Verfahren zur schnellen Wiederherstellung nach schwerwiegenden Vorfällen.  
- \*\*Test-Restore\*\*: Regelmäßige Wiederherstellungstests, um die Integrität der Backups sicherzustellen.  
- \*\*Notfall-Wiederherstellungspläne\*\*: Dokumentation von Vorgehensweisen zur schnellen Reaktion auf Datenverluste.

## 8. Bildquellenverzeichnis

- [Lucidchart Cloud Backup Diagram](https://tse1.mm.bing.net/th?id=OIP.fp\_cvLyUEXsQGYSX6Ok8AQHaHa&pid=Api)  
- [Windows Backup Strategien](https://tse4.mm.bing.net/th?id=OIP.rWt4nt00TTeqBbLD\_DAVvwHaEs&pid=Api)  
- [Backup-Strategie im Unternehmen](https://tse1.mm.bing.net/th?id=OIP.zrNFhcUXJiG6W9Gfho\_oPwHaDt&pid=Api)