Sicherungs- und Wiederherstellungsrichtlinie

Vorlage

**Inhalt**

[Behörde und Überprüfung 3](#_Toc157682628)

[Dokumentenkontrolle und -prüfung 3](#_Toc157682629)

[Versionsverwaltung 3](#_Toc157682630)

[Intro 4](#_Toc157682631)

[Zuständigkeiten 4](#_Toc157682632)

[Verfahren zur Sicherung und Wiederherstellung 4](#_Toc157682633)

[RPO und RTO 5](#_Toc157682634)

[Zugang zu Backup und Verschlüsselung 5](#_Toc157682635)

[Offsite-Sicherung 5](#_Toc157682636)

[Back-up-Überwachung 5](#_Toc157682637)

[Wiederherstellungstest 6](#_Toc157682638)

[ANHÄNGE 7](#_Toc157682639)

[Intro 7](#_Toc157682640)

[ANHANG 1: Zeitplan für die GFS-Sicherung 8](#_Toc157682641)

[Was ist die Großvater-Vater-Sohn-Sicherung? 8](#_Toc157682642)

[Das Prinzip der GFS-Backup-Rotation 8](#_Toc157682643)

[Beispiel für ein G-F-S-Schema 8](#_Toc157682644)

[Schematische Darstellung G-F-S 8](#_Toc157682645)

[Arten von Datensicherungstechniken 9](#_Toc157682646)

[Vollständige Datensicherung 9](#_Toc157682647)

[Inkrementelle Datensicherung 9](#_Toc157682648)

[Differentielle Datensicherung 9](#_Toc157682649)

[Gemischte Datensicherung 9](#_Toc157682650)

[ANHANG 2: 3-2-1-Sicherungsstrategie 10](#_Toc157682651)

[3-2-1-Backup-Regel 10](#_Toc157682652)

[Die Bedeutung der 3-2-1-Regel 10](#_Toc157682653)

[3-2-1-Sicherungsmanagement 11](#_Toc157682654)

[3-2-1 ZUSAMMENFASSUNG 11](#_Toc157682655)

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung** |  |
| Autor |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum der Genehmigung** | **Genehmigt durch** | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

Kritische Informationen und Informationssysteme müssen vor Datenverlust und Datenbeschädigung geschützt werden. Sicherungs- und Wiederherstellungsverfahren ermöglichen die Wiederherstellung von Informationen im Falle von Katastrophenszenarien wie Systemausfällen, Bränden, versehentlicher Löschung oder dem Ausbruch von Malware.

Eine Sicherung ist nicht erforderlich, wenn ein Datenverlust akzeptabel ist oder wenn andere Kontrollmaßnahmen zur Bewältigung von Katastrophensituationen eingesetzt werden. Ein gängiges Beispiel ist ein SPS-System, das eine statische Konfiguration enthält, die im Falle einer Katastrophe leicht wieder eingesetzt oder ersetzt werden kann.

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie **unterstützen**.

# Zuständigkeiten

Der Eigentümer ist für einen effizienten Sicherungs- und Wiederherstellungsprozess verantwortlich, der den Geschäftsanforderungen entspricht. Operative Aufgaben können an Systemadministratoren oder Anbieter delegiert werden.

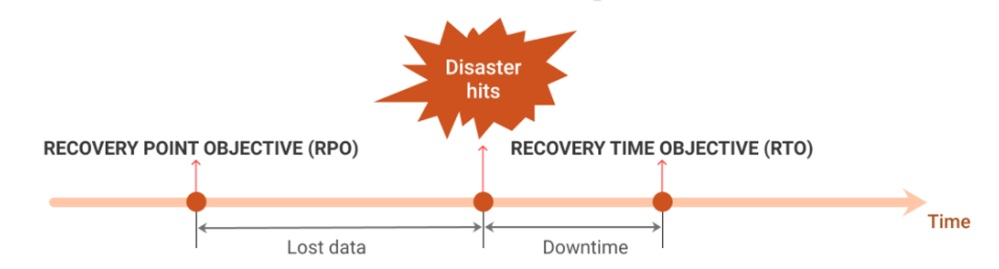
# Verfahren zur Sicherung und Wiederherstellung

Für alle kritischen Systeme muss ein Sicherungs- und Wiederherstellungsverfahren vorhanden sein. Das Sicherungsverfahren sollte die folgenden Themen definieren:

* Welche Informationen werden gesichert (Systeme UND Daten)?
* Erstellung einer Sicherung
* Überwachung von Backups
* Wann und wie oft soll ein Backup durchgeführt werden?
* Wie lange soll die Sicherung aufbewahrt werden?
* Wie und wo soll die Sicherung gespeichert werden?
* Wie werden Sicherungsdaten übertragen?

## RPO und RTO

Das Sicherungsverfahren sollte den geschäftlichen Anforderungen an RPO (Recovery Point Objective) und RTO (Recovery Time Objective) entsprechen, z. B. auf der Grundlage von Risikobewertung und Informationsklassifizierung.



Das RPO definiert den maximalen Zeitraum, in dem Daten aufgrund eines schwerwiegenden Vorfalls verloren gehen können. Wenn zum Beispiel jede Nacht um 2 Uhr eine statische Kopie erstellt wird, beträgt der maximale Datenverlust 24 Stunden.

RTO (Recovery Time Objective) ist die Zeitspanne, die zur Wiederherstellung von Daten benötigt wird.

Verwenden Sie dazu z.B. das GFS-Schema. (**Siehe ANHANG 1: GFS-Backup-Schema.)**

## Zugang zu Backup und Verschlüsselung

Der Zugang zu Backups sollte mindestens das gleiche Schutzniveau haben wie die Originaldaten. Werden vertrauliche Sicherungsdaten physisch oder logisch so gespeichert oder transportiert, dass Unbefugte auf sie zugreifen können, sollten die Daten verschlüsselt werden.

Beispiele hierfür sind:

* Netzwerkverkehr für Backup.
* Sicherungsmedien, die von Personen gespeichert oder übertragen werden, die keinen Zugang zu den Originaldaten haben sollten.
* Backups auf Datenträgern, die an einem Ort aufbewahrt werden der für Personen zugänglich ist, die keinen Zugang zu den Originaldaten haben sollten.
* Der für die Entschlüsselung des externen Datenträgers benötigte Verschlüsselungsschlüssel sollte nicht nur vor Ort aufbewahrt werden.

## Offsite-Sicherung

Um einen Verlust sowohl der Informationen als auch der Sicherungskopie zu vermeiden, sollten die Backups nach Möglichkeit an einem anderen Ort als die Daten selbst aufbewahrt werden. Es sollte eine Übersicht über die ausgelagerten Medien vorhanden sein. Verwenden Sie dazu zum Beispiel die 3-2-1-Sicherungsstrategie. (**Siehe ANHANG 2: 3-2-1-Sicherungsstrategie**)

## Back-up-Überwachung

Der Sicherungsprozess sollte überwacht werden, um den ordnungsgemäßen Betrieb sicherzustellen und Fehler zu beheben. Der ordnungsgemäße Betrieb sollte durch Protokolle, Berichte oder ein automatisiertes System nachgewiesen werden können.

## Wiederherstellungstest

Bei allen für kritische Systeme verwendeten Sicherungsmethoden sollten mindestens einmal jährlich Wiederherstellungstests durchgeführt werden. Eine (ungeplante) Betriebswiederherstellung außerhalb einer geplanten regelmäßigen Testwiederherstellung kann als Wiederherstellungstest gewertet werden.

# ANHÄNGE

## Intro

Beide Diagramme in den folgenden Anhängen können separat eingesetzt werden.

Der **Grandfather-Father-Son** (GFS)-Backup-Plan wird in Umgebungen mit relativ großen Datenmengen oder Systemen verwendet, wenn man nicht genug Zeit hat, um Backups zwischen bestimmten Zeitpunkten durchzuführen und/oder wenn es wichtig ist, weit und detailliert in die Vergangenheit zurückgehen zu können. Dieser Plan berücksichtigt nicht die Backup-Medien oder den Ort der Backups.

Häufig wird das 3-2-1-Schema als Grundlage genommen. Das bedeutet, dass man mindestens drei vollständige Kopien auf zwei verschiedenen Medien hat. Wichtig dabei ist, dass sich eines der verschiedenen Medien an einem anderen Ort befindet. Die 3-2-1-Regel sagt jedoch nichts über das RPO-RTO des Backups aus.

Wie bereits erläutert, können beide Systeme getrennt verwendet werden. Es bietet jedoch einen zusätzlichen Nutzen, wenn beide miteinander kombiniert werden. Das GFS-Schema konzentriert sich auf das RPO-RTO der Daten, während sich die 3-2-1-Strategie auf die Speicherung der erstellten Backups konzentriert.

Das folgende Beispiel verdeutlicht die Anwendung der beiden Prinzipien:

Alle Daten befinden sich auf einem NAS (Network Attached Storage) mit den Festplatten in RAID 10\*. Über einen Backup-Server wird dieses NAS jede Nacht auf einem anderen NAS gesichert. Dieses NAS ist über ein separates Netzwerk mit dem Backup-Server verbunden. Eine vollständige Sicherung der Daten dauert derzeit mehr als 12 Stunden. Um dennoch die sich ändernden Daten zu sichern, wird der GFS-Zeitplan gewählt. Die wöchentlichen und monatlichen Backups werden zusätzlich in eine sichere Cloud-Umgebung kopiert. Auf diese Weise haben wir die 3-2-1-Strategie mit dem GFS-Sicherungsplan kombiniert. [\*https://en.wikipedia.org/wiki/Nested\_RAID\_levels](*https:/en.wikipedia.org/wiki/Nested_RAID_levels)

Die folgende Abbildung zeigt eine schematische Darstellung der oben genannten Erklärung:



## ANHANG 1: Zeitplan für die GFS-Sicherung

### Was bedeutet Großvater-Vater-Sohn-Backup?

Die GFS-Sicherungsrotationstechnik ist eine beliebte **Datensicherungsmethode**, bei der Voll- und Teilkopien auf verschiedenen Medien kombiniert werden können, um sowohl die Sicherungszeit zu verkürzen als auch die Speichersicherheit zu verbessern. Es gibt viele Artikel darüber, was die Großvater-Vater-Sohn-Sicherungsstrategie beinhaltet.

### Das Prinzip der GFS-Backup-Rotation

Bei der Großvater-Vater-Sohn-Sicherungstechnik werden in den drei geplanten Schritten Sicherungen erstellt:

* Der **"Großvater (G)"** - Vollständige Datensicherung für einen bestimmten Standort, einen externen Standort oder mehrere Standorte;
* Der **"Vater (F)"** - ein weiteres vollständiges Backup, regelmäßiger, auf schnellerem Speicher;
* Der **"Sohn (S)"** - inkrementelles Backup (oder differenzielles Backup) auf demselben Speicher wie der "Vater".

### Beispiel für ein GFS-Schema

Der GFS-Zeitplan beginnt mit den **täglichen Backups**. Normalerweise gibt es vier Sicherungsmedien die mit dem Tag der Woche gekennzeichnet sind an dem sie gesichert werden, z. B. von Montag bis Donnerstag. Jedes Medium wird an dem beschrifteten Tag zur Verwendung aufgerufen. Wenn nur eine einwöchige Versionshistorie der Dateien geführt wird, wird jedes Medium jede Woche überschrieben. Um eine 3-wöchige Versionshistorie von Dateien zu führen (empfohlen), werden mehr Medien benötigt. Das Montagsmedium einer Woche wird dann zum Beispiel erst 3 Wochen später überschrieben.

**Wöchentliche Sicherungen** folgen einem ähnlichen Szenario. Ein Satz von bis zu fünf wöchentlichen Sicherungsmedien wird mit "Woche 1", "Woche 2" usw. gekennzeichnet. Vollständige Sicherungen werden wöchentlich an dem Tag aufgezeichnet, an dem ein "Sohn"-Medium nicht verwendet wird. Im obigen Beispiel wären dies die "Freitag"-Medien. Dieses "Vater"-Medium wird monatlich wiederverwendet. Für eine einmonatige Dateihistorie werden fünf wöchentliche Medien benötigt, da manche Monate 5 Wochen haben.

Der letzte Satz von drei Medien wird mit "**Monat1**", "Monat2" usw. gekennzeichnet, je nachdem für welchen Monat des Quartals sie verwendet werden. Dieses "Großvater"-Medium zeichnet vollständige Sicherungen am letzten Arbeitstag eines jeden Monats auf. Wenn Ihr Sicherungsplan einem steuerlichen Geschäftskalender folgt, ersetzt Ihr Monatsmedium das Wochen-/Vaterband der Woche 4 oder der Woche 5, je nach Monat. Richtet sich Ihr Sicherungsplan nach Kalendermonaten, dann wird Ihre monatliche Sicherung im Laufe des Jahres variieren und ein tägliches oder wöchentliches Medium ersetzen. In der Regel werden die monatlichen Medien vierteljährlich oder jährlich (empfohlen) überschrieben, je nach den Anforderungen an die Versionshistorie.

### Schematische Darstellung GFS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Woche 1** |
| **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Woche 2** |
| **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Woche 3** |
| **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Monat1** |

### Arten von Datensicherungstechniken

Jede Dateisicherungssoftware bietet mindestens eine Datensicherungsmethode an, die Vollsicherung, bei der ein ganzer Datensatz auf ein endgültiges Medium kopiert wird. Es gibt jedoch auch andere Arten der Datensicherung, oft um Zeit und Platz für regelmäßige Backups zu sparen. Diese Sicherungsarten sind:

* **Vollständige Sicherung** - vollständiges Kopieren der Daten wie oben beschrieben;
* **Teil-Sicherung** - kopiert nur Daten, die seit der letzten Sicherung geändert wurden:
  + **Inkrementelle Sicherung** - kopiert nur Daten, die nach der letzten inkrementellen Sicherung geändert wurden
  + **Differenzielle Sicherung** - kopiert nur Daten, die nach der letzten Vollsicherung geändert wurden
* **Gemischte Sicherung** - eine Folge von Vollsicherungen und einigen Teilsicherungen, die wiederholt rotiert werden:
  + **Gemischte inkrementelle Sicherung** - eine Kette von vollständigen und einzelnen inkrementellen Sicherungen;
  + **Gemischte differentielle Sicherung** - ein Satz von vollständigen und einzelnen differentiellen Sicherungen.

Die Vollsicherung ist die Grundlage für jede differenzielle oder inkrementelle Sicherung sowie für gemischte Sicherungen.

### Vollständige Datensicherung

Bei einer Vollsicherung wird davon ausgegangen, dass jedes Mal wenn die Aufgabe ausgeführt wird, der gesamte Datensatz an den gewählten Speicherungsort kopiert wird. Eine Vollsicherung nimmt viel Platz, Zeit und PC-Ressourcen in Anspruch, und erstellt oft viele unnötige Datenkopien, da die meisten Daten im Datensatz zwischen den Sicherungen nicht verändert werden.

### Inkrementelle Datensicherung

Bei der inkrementellen Sicherung werden nur Dateien verarbeitet, die seit der letzten inkrementellen Sicherung neu hinzugekommen sind oder sich verändert haben. Nach einer anfänglichen Vollsicherung ist jede nachfolgende Sicherung inkrementell und speichert nur den Unterschied zwischen dem aktuellen Datensatz und einer vorherigen inkrementellen Kopie.

### Differentielle Datensicherung

Die differenzielle Sicherung ist der inkrementellen Sicherung sehr ähnlich, verwendet aber andere Datensicherungsstrategien. Nach einer anfänglichen Vollsicherung ist jede nachfolgende Sicherung inkrementell und speichert nur den Unterschied zwischen dem aktuellen Datensatz und einer vorherigen vollständigen Kopie.

### Gemischte Datensicherung

Dieser Ansatz ist eine Kombination aus zwei verschiedenen Arten von Backups: vollständige und partielle (inkrementelle oder differentielle) Backups. Sie ähnelt auch einer versionierten Sicherungstechnik. Bei dieser Methode wird eine Vollsicherung durchgeführt, gefolgt von einer festen Anzahl von Teil-Sicherungen.

## ANHANG 2: 3-2-1-Sicherungsstrategie

Die **3-2-1-Sicherung** ist eine bewährte Methode zum Schutz und zur Wiederherstellung von Daten, mit der sichergestellt wird, dass die Daten angemessen geschützt sind und bei Bedarf aktuelle Sicherungskopien der Daten zur Verfügung stehen. Das Grundkonzept der 3-2-1-Backup-Strategie besteht darin, drei Backups der zu schützenden Daten zu erstellen, die Backups auf zwei verschiedenen Arten von Speichermedien zu sichern und ein Backup der Daten an einen anderen Ort zu senden.

Im klassischen 3-2-1-Sicherungsszenario wird eine Sicherungssoftware zur Sicherung unternehmenskritischer Daten verwendet, wobei die Sicherung der Daten auf einem anderen Datenspeichergerät vor Ort gespeichert wird. Während dieses Prozesses oder unmittelbar danach werden zwei weitere Sicherungen der Daten auf zwei anderen Geräten gespeichert; traditionell war mindestens eines dieser Geräte eine Bandbibliothek. Das Band war ein Standardbestandteil des Prozesses, weil es einfach war, eine tragbare Sicherung der Daten in Form einer Bandkassette zu erstellen, die leicht an einen anderen Ort transportiert werden konnte. In vielen Umgebungen ist das Band jedoch durch ein Festplattenspeichersystem ersetzt worden.

Obwohl der 3-2-1-Sicherungsansatz schon seit Jahrzehnten ein Eckpfeiler der Datensicherung in großen und kleinen Rechenzentren ist, wird dieses Konzept von den meisten Anbietern von Sicherungssoftware und -hardware nach wie vor als "Best Practice" für den effektiven Einsatz ihrer Produkte angesehen. Die Anbieter geben zu, dass das allgemeine Konzept immer noch gültig ist, unabhängig davon, wie oder wo ein Unternehmen seine Daten speichert - auch wenn neue Anforderungen und Big Data die 3-2-1-Gleichung etwas komplizierter gemacht haben.

### 3-2-1-Backup-Regel

Die 3-2-1-Sicherungsstrategie besteht aus drei Regeln:

* **Drei Datenkopien**. Von allen kritischen Daten sollten regelmäßig - täglich oder öfter - drei Sicherungskopien angefertigt werden, darunter die Originaldaten und mindestens zwei Sicherungskopien.
* **Zwei Arten der Speicherung.** Für die Speicherung der Daten sollten zwei verschiedene Speichertypen verwendet werden. Beide Kopien der Sicherungsdaten sollten auf zwei verschiedenen Speichertypen gespeichert werden, um das Risiko eines Ausfalls zu minimieren. Zu den Speichergeräten können eine interne Festplatte, eine externe Festplatte, ein Wechseldatenträger, eine Bandbibliothek, ein sekundäres Speicher-Array oder eine Cloud-Sicherungsumgebung gehören.
* **Ein Speicherort außerhalb des Unternehmens**. Eine Kopie der Sicherungsdaten sollte an eine externe Speichereinrichtung geschickt werden. Mindestens eine Datenkopie sollte an einem externen Standort aufbewahrt werden, um sicherzustellen, dass Natur- oder geografische Katastrophen nicht alle Datenkopien beeinträchtigen können. Diese Kopie kann, wie bei bandgestützten Sicherungen, physisch an den externen Standort geliefert oder über Telekommunikationseinrichtungen anm sekundären Standort repliziert werden.

### Die Bedeutung der 3-2-1-Regel

Die 3-2-1-Backup-Strategie gilt als "Best Practice" für Fachleute für Informationssicherheit und Datenschutz. Das Verfahren garantiert zwar nicht, dass alle Daten niemals in irgendeiner Weise gefährdet sind, aber die Strategie beseitigt einige der mit Sicherungsverfahren verbundenen Risiken. Die 3-2-1-Methode ist wichtig, um sicherzustellen, dass es keinen einzigen Ausfallpunkt für Daten gibt. Ein Unternehmen ist mit dieser Methode nicht nur dann abgesichert, wenn eine Kopie beschädigt wird oder eine Technologie ausfällt, sondern auch bei einer Naturkatastrophe oder einem Diebstahl, der die physischen Speichermedien zerstört.

Der Datenwiederherstellungsprozess mit der 3-2-1-Methode sieht folgendermaßen aus:

* Die (aktiven) Originaldaten wurden beschädigt oder sind verloren gegangen. Wenn die Produktionskopie der Daten nicht verfügbar ist, besteht die erste Alternative darin, die benötigten Daten aus der intern auf einem anderen Medium oder einem sekundären Speichersystem gespeicherten Sicherungskopie wiederherzustellen.
* Die zweite Datenkopie ist nicht verfügbar oder unbrauchbar. Wenn das System - Band oder Festplatte -, auf dem die zweite Datenkopie gespeichert ist, nicht verfügbar ist, oder wenn die Datenkopie beschädigt, veraltet oder anderweitig unbrauchbar ist, muss die externe Kopie auf den internen Servern abgerufen werden.
* Starten Sie den 3-2-1-Prozess so bald wie möglich neu. Sobald eine geeignete Datenkopie angeschlossen und der Betrieb wiederhergestellt ist, sollte der Sicherungsprozess so schnell wie möglich neu gestartet werden, um sicherzustellen, dass die Daten weiterhin angemessen geschützt sind.

Heutzutage sind Sicherungskopien nicht mehr nur Versicherungspolicen die vergessen werden bis etwas schief geht. Unternehmen können den Wert ihrer Backup-Datenspeicher steigern, indem sie diese Daten beispielsweise für die Entwicklung und das Testen neuer Anwendungen nutzen. Zeitgemäße Programmieransätze wie DevOps erfordern einen einfachen Zugriff auf Daten, die so nah wie möglich an den Live-Anwendungsdaten liegen, um sicherzustellen, dass die Anwendungen angemessen für eine reale Umgebung entwickelt werden. Backup-Daten erfüllen diese Anforderung perfekt, da sie wahrscheinlich regelmäßig und häufig neu generiert werden.

Analytische Anwendungen benötigen möglicherweise auch Zugang auf großen Mengen aktueller Daten. Durch die Verwendung frischer Sicherungsdaten sind die Ergebnisse des Analyseprozesses wahrscheinlich zuverlässiger und genauer. Strengere Kontrollen und die Verwaltung von Datenunternehmen sind erforderlich, um sicherzustellen, dass diese Anwendungen die bestmöglichen Daten erhalten, während die primären Konzepte der 3-2-1-Sicherung beibehalten werden. Wenn eine der Sicherungskopien für die Anwendungsentwicklung oder -analyse verwendet wird, kann sie verändert werden oder nicht mehr verfügbar sein, wodurch eine der drei erforderlichen Kopien unbrauchbar wird, wenn eine Wiederherstellung erforderlich ist.

Die Datenintegrität war schon immer ein zentrales Anliegen bei der Datensicherung. Es reicht nicht aus, nur Daten zu sichern und die Kopien wegzusperren; es muss auch sichergestellt werden, dass die Sicherungen vollständig, unbeschädigt und wiederherstellbar sind. Wiederherstellungstests helfen dabei, ebenso wie die Verwendung einiger der fortschrittlicheren Funktionen, die Backup-Software zur Erkennung von Ransomware und anderen Bedrohungen bieten. Auch diese Bedenken stehen einem 3-2-1-Backup-Konzept nicht unbedingt im Wege, können aber den Prozess um einige Schritte erweitern, z. B. durch regelmäßige Wiederherstellungstests.

### 3-2-1-Sicherungsmanagement

Es gibt einige grundlegende Prinzipien für eine erfolgreiche 3-2-1-Backup-Implementierung:

* Alle Datenkopien sind identisch und aktuell.
* Die Medien, auf denen die Kopien gespeichert sind, sind lesbar.
* Alle Proben und Geräte werden getestet und ihre Funktionstüchtigkeit bestätigt.
* Fernkopien werden sicher gespeichert.
* Die Wiederherstellung von einzelnen/mehreren Dateien oder einer vollständigen Sicherung wird regelmäßig getestet.
* Interne Datenkopien befinden sich auf verschiedenen Speichersystemen und Netzen und können von außerhalb des Unternehmens nicht eingesehen werden.

Die im 3-2-1-Verfahren eingesetzte Sicherungssoftware kann sehr nützlich sein, da sie die Anordnung der Sicherungskopien automatisch steuern und alle Sicherungsaktivitäten katalogisieren kann. Die meisten solcher Software haben auch Funktionen zur Prüfung auf Bedrohungen wie Malware, Ransomware und Viren in den Sicherungskopien hinzugefügt.

### 3-2-1 ZUSAMMENFASSUNG

3 Kopien der Daten

2 verschiedene Medien

1 Kopie außerhalb des Unternehmens

Bewahren Sie die Daten auf mindestens **2 Arten von Speichermedien auf**.  
(Lokale Festplatte, NAS, Band,...)

**Speichern Sie 1 davon außer Haus** (sicherer Speicher, Cloud,...)

Erstellen Sie **3 Kopien** der Sicherungsdaten.   
 (1 primäre und 2 Sicherungskopien