SAY**FUSE** Backup & Restore Plattform

# Datensicherungskonzept

SAYTEC

## Inhaltsverzeichnis

# 1. Vorwort

Eine verlässliche Datensicherung erfordert immer ein bedarfsgerechtes Sicherheitskonzept. Jederzeit können durch technisches Versagen, Anwenderfehler, Angriffe oder Manipulationen Unternehmensdaten verloren gehen, Serversysteme zusammenbrechen und Archive unbrauchbar werden. Im Schadensfall müssen gesicherte Daten – durch den redundanten Bestand – wiederhergestellt und die Betriebsaufnahme sichergestellt werden. Untersuchungen zeigen, dass bis zu 70 Prozent der Unternehmen nach einem Störfall oder Angriff ihre Daten nicht wiederherstellen konnten. Eine Vielzahl der Sicherheitskonzepte hat versagt. Dies kann auf die Inkonsistenz zwischen verschiedenen Speichersystemen, Technologien oder auf einen zerstörten Datensatz zurückgeführt werden. SAYTEC hat sich dieser Herausforderung gestellt und eine hochsichere Back-up-, Storage- und  Restore-Plattform entwickelt. Sie erfüllt alle technischen und gesetzlichen Anforderungen an eine wirksame und verlässliche Datensicherung.

Das Produktivnetzwerk und die daraus resultierenden Einflussfaktoren bestimmen die Vorgehensweise bei der Datensicherung. Zu den Einflussfaktoren gehören die eingesetzten Serversysteme, die Datenmengen, die Datenbanken und die Änderungsfrequenz derselben. Die Verfügbarkeitsanforderungen und der Auslagerungsrhythmus der Datensicherung gehören ebenfalls zu den wichtigen Faktoren. Das Datensicherungskonzept berücksichtigt all diese Faktoren und behandelt neben der Datensicherung auch die IT-Infrastruktur. Für die Realisierung sind geeignete Hardware- und Softwarelösungen zu bestimmen, die ihre Funktionen regelmäßig unter Beweis stellen müssen.

Das reibungslose Funktionieren der Datensicherung sowie die Wiederherstellbarkeit der Daten erfordern die Umsetzung praktischer Aufgaben. Diese müssen nachvollziehbar dokumentiert und regelmäßig durchlaufen werden.

## 2. Zielsetzung

Das Ziel eines Datensicherungskonzeptes (basierend auf der vorhandenen Infrastruktur) ist die Sicherstellung der Verfügbarkeit der Daten sowie die Ausfallsicherheit der Serversysteme. Dabei sollen heutige und zukünftig zu erwartende Anforderungen bestmöglich erfüllt werden. Das Konzept muss physische und virtuelle Umgebungen sowie die Verarbeitung großer Datenmengen unterstützen und diese bei Bedarf bereitstellen.

Eine ideale Lösung erfordert periodische Vollsicherungen nach dem Generationsprinzip und die Auslagerung des gesicherten Datenbestandes in einen anderen Brandabschnitt. Die Backup- und Restore-Plattform muss daher schnell und einfach skalierbar sein, damit sie nicht zum Flaschenhals wird. Wichtig sind natürlich auch Informationen über die Skalierungssystematik und die maximal erreichbare Größe der Plattform. Ein kritischer Teil der Datensicherheitsstrategie ist die Unveränderbarkeit der Backups durch Dritte und durch Ransomware.

Die Datensicherung ist heute nicht nur als Sicherung von Daten anzusehen. Sie ist mittlerweile eine Art Versicherung gegen Verlust der Betriebsfähigkeit. Immer häufiger entstehen neue Anforderungen, die die Backup- und Restore-Plattform erfüllen muss. Dazu gehören bspw. die Archivierung, Test-/VM-Umgebungen und Migrationen. Gleichzeitig dürfen die neuen und oftmals sekundären Anwendungsfälle den primären Zweck nicht beeinträchtigen. Eine verlässliche und schnelle Wiederherstellung muss stets gewährleistet sein.

## 3. Soll-Zustand

Auf Grund stetig zunehmender Datenvolumen und Anforderungen an IT-Systeme ist eine konsistente Datenschutzstrategie unerlässlich. Die Nichtverfügbarkeit der Daten und der Ausfall der IT-Systeme würden einen sehr großen Schaden verursachen.

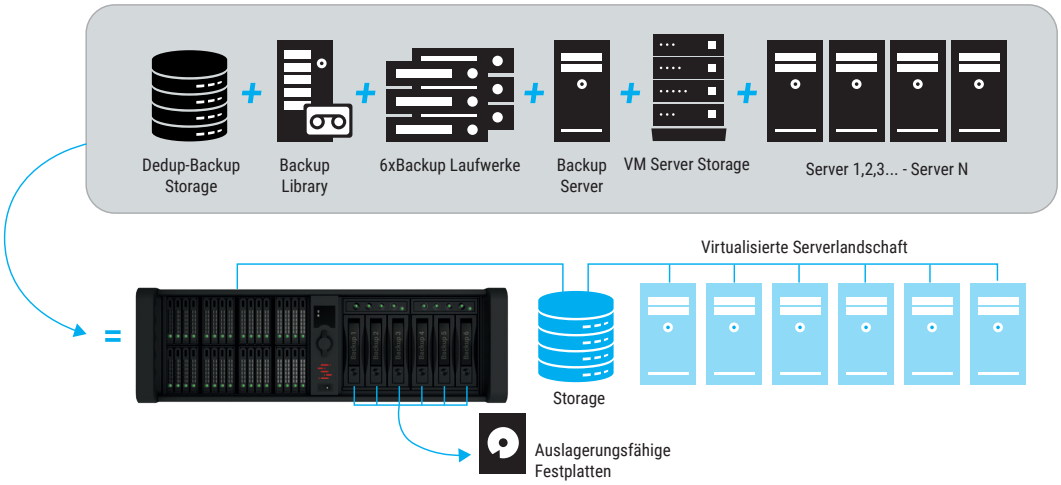
Im Sollzustand sorgt die SAY**FUSE** Appliance als Backup-Restore-Plattform nicht nur bei Primär- und Sekundärsicherungsvorgängen, sondern auch bei Sekundäranwendungsfällen für Ausfallsicherheit, Verfügbarkeit und unmittelbare Bereitstellung der kritisch definierten Infrastrukturen. Bei Bedarf können zwei SAY**FUSE** Appliances miteinander geclustert werden. Die SAY**FUSE** Plattform ist so konzipiert, dass alle Compliance-Richtlinien innerhalb des Systems (ohne weitere Hard- und Software) erfüllt werden. So wird die IT-Infrastruktur sicherer, die Bedienung einfacher, und die Betriebskosten reduzieren sich signifikant.

Die SAY**FUSE** Backup Plattform erfüllt alle vier grundlegenden Stufen einer zuverlässigen Sicherungsstrategie in einer Appliance.

# 4. Das Konzept

## 4.1. Die SAYFUSE Backup- und Restore-Plattform

Durch die Implementierung der SAY**FUSE** Backup-Restore-Plattform wird bei Unternehmen die Datensicherheit gewährleistet. Die Backup- und Restore-Plattform sieht primäre und sekundäre Sicherungsvorgänge sowie sekundäre Anwendungsfälle vor. Dadurch erfüllt SAY**FUSE** die Anforderungen an Ausfallsicherheit, Verfügbarkeit, Datensicherung, Auslagerung und Wiederherstellung. Mit der Erneuerung durch die Backup- und Restore-Plattform wird das bestehende Konzept soweit optimiert, dass die Anforderung an die Datensicherung erfüllt und die Ausfallsicherheit gewährleistet ist.




## 4.2. Primär- und Sekundär-Sicherungsvorgänge und sekundäre Anwendungsfälle

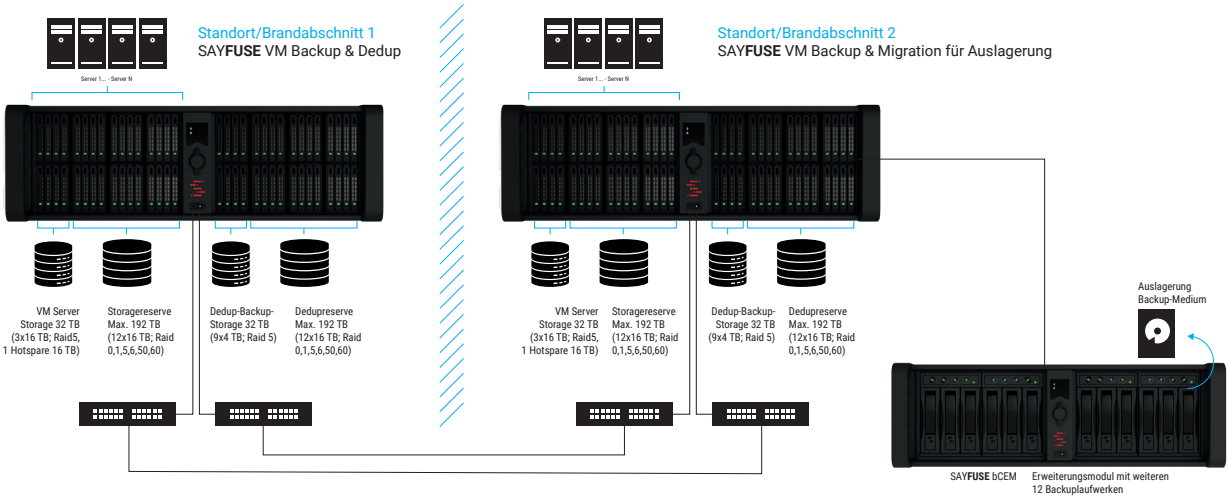
Das Konzept sieht einen Primär- und Sekundär-Sicherungsvorgang sowie sekundäre Anwendungsfälle vor. So können kritisch gekennzeichnete Systeme bei einem Ausfall unmittelbar als sekundäres Anwendungssystem aus dem SAY**FUSE** gestartet und für die Nutzung freigegeben werden.

Der Primär-Sicherungsvorgang erfolgt z.B. im Brandabschnitt 1 / Rechenzentrum 1 vom Netzwerk in den Backup- oder Dedup-Storage im SAY**FUSE**. Diese Datensicherung erfolgt täglich als erste Sicherungsstufe. Hier werden tägliche Sicherungen mindestens eine Woche lang vorgehalten und dienen der unmittelbaren Wiederherstellung der Daten oder Systeme. Ferner können einzelne Server bei Ausfall unmittelbar von hier aus wiederhergestellt werden.

Der Sekundär-Sicherungsvorgang erfolgt kontinuierlich als Migration, ohne die Netzwerkressourcen (und den Betrieb der kritischen Systeme) zu belasten. Innerhalb der SAY**FUSE**-Appliance werden durch Migration die Wochen- und Monatssicherungen als vollständige Sicherungsdatensätze erzeugt. Diese können per Knopfdruck entfernt und an einen sicheren Ort ausgelagert werden.

Im Sekundär-Sicherungsvorgang kann die Migration aus dem Backup-/Dedup-Storage des Primären-Sicherungsvorgangs auch in ein anderes im Brandabschnitt 2 / Rechenzentrum 2 befindliches SAY**FUSE** erfolgen.

SAY**FUSE** Backup
Konzept: Dedup & Migration + Ausfall & Verfügbarkeit




Eine logische Aufteilung der Datensicherung nach Sicherungs-LUNs (nach Daten, VMs und kritische Server-Systeme) ermöglicht eine flexible und schnelle Reaktionsfähigkeit. So können einzelne Systeme aus der Primärsicherung gestartet oder wiederhergestellt werden. Das ausgefallene System kann angeschafft bzw. repariert werden.

## Der sekundäre Anwendungsfall - die sofortige Reaktionsfähigkeit

Die kritischen Systeme können unmittelbar aus der SAY**FUSE** Appliance in Betrieb genommen werden; z.B. bei einem Totalausfall der Serversysteme (Hardware und Software). Die als kritisch definierten Serversysteme werden im SAY**FUSE** offline bereitgehalten und täglich aktualisiert. Tritt ein Ausfall eines kritischen Servers ein, wird dieses System innerhalb weniger Minuten aus dem SAY**FUSE** bereitgestellt. So wird eine maximale Verfügbarkeit und Ausfallsicherheit für kritische Infrastrukturen erreicht.

Mindestens die Monatssicherung sollte eine vollständige Sicherung des gesamten

Netzwerkes, der Server sowie der Daten beinhalten. Die monatliche Sicherung sollte mindestens 6, besser 12 Monate aufbewahrt werden. Nach Ablauf des Aufbewahrungszeitraums können die Medien wiederverwendet werden.

An einem zweiten Standort wird die zweite Backup- und Restore-Plattform an ein SAY**FUSE** Kapazitätserweiterungsmodul (bCEM) angeschlossen. 18 Backuplaufwerke mit jeweils 14 TB Backupmedien (unkomprimiert) werden für die Migration der Sicherungen aus dem SAY**FUSE** Backup Dedup Store des ersten Rechenzentrums in das zweite Rechenzentrum verlagert. Aktuell können mit dieser Konfiguration unkomprimiert 252 TB ausgelagert werden.

Die Aktualisierung/Upgrade des SAY**FUSE** Backup Systems durch die neue Backup- und Restore-Plattform hat den Vorteil, dass die bisherigen Backupmedien auch bei zukünftigen Erweiterungen nicht aufwändig migriert werden müssen. Die SAY**FUSE** Technologie ist aufwärts und abwärts kompatibel, das erlaubt die Weiternutzung bisher verwendeter Medien bzw. die Wiederherstellung von den darauf befindlichen Sicherungen.

Das Konzept unterstützt physische und virtuelle Umgebungen. So werden auch größere Datenmengen verarbeitet und bei Bedarf bereitgestellt. Zudem ist die Backup- und Restore-Plattform jederzeit schnell und einfach skalierbar um für zukünftig steigende Anforderungen gerüstet.

Die SAY**FUSE** Backup- und Restore-Plattform steht auch für zusätzliche Anwendungsfälle zur Verfügung, ohne dass die sekundären Anwendungsfälle den primären Zweck beeinträchtigen. Dazu zählen Archivierung, Test- und VM-Umgebungen, Migrationen, virtuelle Server und weitere Storages.

München, 2019

SAYTEC AG

# 5. Anlagen

## 5.1. Entwicklung des neuen Datensicherungskonzepts (Erneuerung, Aktualisierung Ihres bestehenden SAYFUSE Systems)

Mit der Aktualisierung Ihres SAY**FUSE** Backup Systems wird Ihr bestehendes Datensicherungskonzept um  die neuen Funktionen der Backup- und Restore-Plattform erweitert.

Die neue SAY**FUSE** Plattform bietet Ihnen wichtige Alleinstellungsmerkmale. Die Datensicherung und Wiederherstellung mit sehr hoher Geschwindigkeit sorgen stets für Ausfallsicherheit und Verfügbarkeit der geschäftskritischen Systeme. Für die optimale Implementierung sind folgende Punkte zu klären:

**Erfassung und Priorisierung**

- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Business Continuity, kritische Systeme
- Vollsicherung, inkrementelle Datensicherung, Migration und Auslagerung
- Clusterknoten auf der SAY**FUSE** Plattform für Ausfallsicherheit und Verfügbarkeit

**Gefährdungslage**

- Abhängigkeit, die Aufrechterhaltung und Existenz des laufenden Geschäftsbetriebes (Datenbestand und Verfügbarkeit der IT-Systeme)
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Medienfehler
- Institutionsrelevante Schadensursachen
- Schadenfälle im eigenen Haus

**Einflussfaktoren je IT-System**

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten

- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

**Datensicherungsplan IT-System**

- Sinnvolle Gruppierung der Sicherung in logische Jobs
- Prioritätserfassung in Abhängigkeit der Betriebsfortführung

**Festlegungen je Daten-Art**

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

**Festlegung der Vorgehensweise für den Restore-Fall**

- Randbedingungen für das Datensicherungsarchiv
- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von gesicherten Daten
- Vernichtung von unbrauchbaren Datenträgern
- Vorhalten von arbeitsfähigen Lesegeräten

**Minimaldatensicherungskonzept**

Es muss ein Minimaldatensicherungskonzept erstellt werden, das die Mindestanforderungen für die Datensicherung festlegt. Dazu zählen Beschreibungen, wie die Datensicherung erfolgt, wie Daten wiederhergestellt werden können, welche Parameter gewählt wurden und welche Hard- und Software eingesetzt wird.

**Verpflichtungen der Mitarbeiter bei der Datensicherung,**
**Sporadische Restore-Übungen**

Ein Unternehmen sichert regelmäßig seine wichtigen Daten, vor allem seine Kundendaten. Wenn jedoch nicht regelmäßig getestet wird, ob sich die Daten wieder einspielen lassen, können im Störfall möglicherweise gesicherte Daten nicht wiederhergestellt

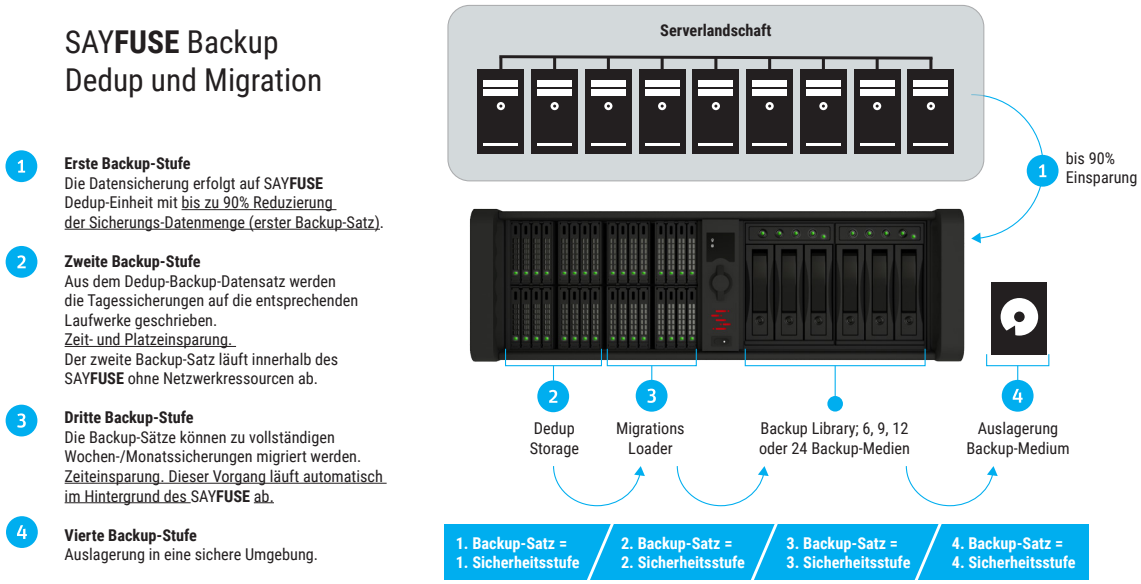
werden oder nicht mehr nutzbar sein. Sind Kundendaten betroffen, so kann dies zu erheblichen Schäden führen, bis hin zur Einstellung des Vertriebs.

### Prüffragen

- Wird der Restore-Fall regelmäßig getestet?
- Sind die betroffenen IT-Systeme im Datensicherungskonzept aufgeführt?
- Sind die verantwortlichen Mitarbeiter über Details beziehungsweise Teile des Datensicherungskonzepts unterrichtet?
- Wird die Umsetzung des Datensicherungskonzepts regelmäßig kontrolliert?
- Ist die Auslagerung des Datenbestandes und der Systeme gewährleistet?

## 5.2. Das Generations-Sicherungskonzept in vier Stufen

Die Sicherung und Wiederherstellung mit der SAY**FUSE**-Appliance durch Multi-Backup-Laufwerke, Multi-Stream und Migration erhöht die Geschwindigkeit überdurchschnittlich. Viele Terabytes an Daten können innerhalb weniger Stunden gesichert und in eine geschützte Umgebung auslagert werden.




### Stufe 1

In der ersten Stufe beginnt die Datensicherung mit einer echten vollständigen Sicherung in das Backup-Dedup-Storage innerhalb des SAY**FUSE**. Dies spart Zeit, reduziert die Netzwerkbelastung bis zu 90% und bildet den ersten Sicherungsdatensatz.

**Stufe 2**
In der zweiten Stufe wird jobgesteuert das dafür konfigurierte Backuplaufwerk eingeschaltet und die Tagessicherungen werden innerhalb der SAY**FUSE** Appliance aus dem Backup-/Dedup-Pool auf die entsprechenden Medien migriert. Nach Abschluss der Sicherung wird das Sicherungslaufwerk abgeschaltet. Dieser Vorgang findet ohne externen Zugriff statt, spart Zeit und schont die Netzwerkressourcen.

**Stufe 3**
In der dritten Stufe migrieren die Backup-Sätze automatisch im Hintergrund (innerhalb der Appliance) mit den täglichen Änderungen in die wöchentlichen bzw. monatlichen Vollsicherungen. Dabei werden die jeweils dafür konfigurierten Backup-Laufwerke mit dem Backup-Job eingeschaltet und die Backupmedien auf Konsistenz geprüft. Nach Abschluss der Sicherung wird das jeweilige Backup-Laufwerk abgeschaltet und die Sicherung für die Auslagerung bereitgestellt. Das schützt die Sicherung vor Angriffen, spart Energie und erhöht die Lebensdauer der gesicherten Daten.

**Stufe 4**
Die Auslagerung ist die vierte Stufe. Auf Knopfdruck können Sicherungsmedien als Voll-Sicherungssätze aus den Sicherungslaufwerken entfernt und in eine geschützte Umgebung ausgelagert werden.

Die Datensicherung ist nach dem Generationsprinzip (Großvater, Vater, Sohn) sinnvoll. Normalerweise macht sich der Verlust von Daten erst nach einiger Zeit bemerkbar. Durch datenbankgesteuerte Sicherungen nach dem Generationsprinzip können Daten oder Gesamtsysteme eines länger zurückliegenden Zeitpunkts wiederhergestellt werden.

Bei dieser Methode werden die Backupmedien wie folgt überschrieben:
1. die Tagessicherungen, zum jeweiligen Tag der Folgewoche
2. die Wochensicherungen, zur jeweiligen Woche des Folgemonats
3. die Monatssicherungen, zum jeweiligen Monat des Folgejahres.

Somit wird die Rückverfolgung für ein ganzes Jahr (mit 21 Medien) sichergestellt.

## 5.3 Datenübertragungskapazitäten

Die Datenübertragungskapazität, d.h. die Menge der digitalen Daten, die über einen bestimmten Zeitraum in einem Übertragungskanal transportiert werden, hängt von vielen Faktoren ab. Für ein durchgängiges Backupkonzept müssen sämtliche Faktoren berücksichtigt werden. Für die Sicherung großer Datenmengen, deren Replikation und Auslagerung müssen alle Schnittstellen, die Topologie sowie Storage- und Sicherungslaufwerke für die Auslagerung berücksichtigt werden.

Im Zeitalter großer Datenmengen ist es uns möglich, 100 TB Daten oder mehr an einem Tag oder Wochenende auszulagern und für die Rücksicherung verfügbar zu machen.

## SAY**FUSE** Backup
## Datenübertragungskapazität