FAST LTA
Wir sichern Petabytes.

Sekundärspeicher für Backup und Archivierung:

Die 3 Ebenen der Datensicherung

Datensicherung ist der Überbegriff für alle Maßnahmen, die dem Verlust von Daten vorbeugen sollen. Ziel der Datensicherung ist es, angeforderte Daten jederzeit in der originär abgelegten Form bereitstellen zu können. Da Primärspeicher limitiert und teuer sind, werden zur Datensicherung Sekundärspeicher eingesetzt. Hauptanforderung an solche Systeme für Backup und Archivierung ist die langfristige, sichere und kostengünstige Speicherung großer Datenmengen.

Die möglichen Ursachen für Datenverlust - und damit auch die Präventivmaßnahmen - lassen sich in drei Ebenen anordnen.

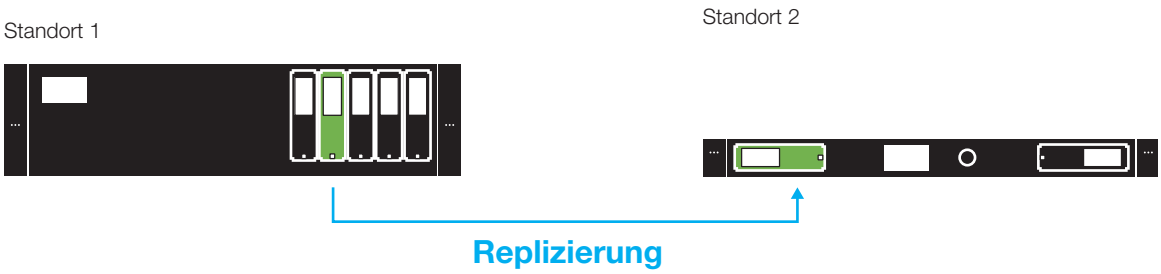
Stand: Februar 2019

1. Die System-Ebene

Der augenscheinlichste Grund für Datenverlust: Das System, das die Daten gespeichert hat, ist unrettbar defekt oder nicht mehr verfügbar. **Katastrophen** (Feuer, Wasser), aber auch **Diebstahl** und mutwillige Zerstörung sind Ursachen dafür. In komplexen Systemen kann es aber auch ausreichen, wenn entscheidende Komponenten den Dienst quittieren. Ein Umzug von Daten von einem defekten auf ein intaktes System ist, wenn überhaupt, oft nur mit erheblichem Aufwand möglich.

Sind bei einem Speichersystem Infrastruktur und Medien getrennt, können diese im Fall eines Systemausfalls in einem Ersatzsystem wieder eingelegt und gelesen werden. Ein Systemausfall hat also keinen Einfluss auf die Datensicherheit.

Grundsätzlich ist ein zweites System, das sich an einem separaten Standort befindet, geeignet, bei einem Systemausfall schnell wieder für Verfügbarkeit der Daten zu sorgen. Die Umschaltung zwischen System kann dabei automatisch (Fail Over) oder manuell erfolgen. Üblicherweise muss das Zweitsystem eine exakte Kopie des Hauptsystems sein, auf dem alle Daten gespiegelt abgelegt werden. Manche Systeme erlauben eine selektive Spiegelung von Datenbereichen, oder eine **Replizierung** von Datenträgern, die sich auch über mehrere Instanzen erstrecken kann.



Die Replizierung von Daten zu einem zweiten Standort schützt vor Datenverlust durch Totalausfall.

2. Die Hardware-Ebene

Um sich gegen Datenverlust durch den Ausfall einzelner Komponenten zu schützen, setzt man **Redundanz** ein. Dies gilt für Netzteile, Netzwerk-Schnittstellen, aber speziell auch für Datenträger.
Die einfachste Methode ist auch hier die Spiegelung.

Robin Harris: Why RAID 5 stops working in 2009 – https://www.zdnet.com/article/why-raid-5-stops-working-in-2009/

Um mehr als einen Ausfall zu kompensieren, haben sich Redundanz-Codierungen zur Absicherung etabliert - die bekanntesten sind **RAID-5** und **RAID-6**, die einen Verbund mit einem bzw. zwei zusätzlichen Datenträgern absichern. Nicht nur aufgrund dieser geringen Redundanz sind die genannten RAID-Versionen jedoch **nicht für die langfristige Sicherung** geeignet, auch wenn sie für Primärspeicher einen guten Kompromiss zwischen Aufwand und Kosten darstellen. Problematisch ist vor allem das Verhalten im Fehlerfall - also genau der Fall, vor dem RAID schützen soll. Einerseits sind die benötigten Systemressourcen für die Wiederherstellung defekter Datenträger ziemlich hoch, was den Speicher im Betrieb verlangsamt. Andererseits werden Fehler, die bei der Speicherung auch “unentdeckt” über die Lebensdauer der Datenträger (unrecoverable errors - URE) entstehen können, erst beim Lesen (und demnach beim Rebuild) entdeckt. Die meisten Systeme brechen den Rebuild dann ab, die ursprünglich gewünschte Sicherheit kann nicht wiederhergestellt werden. Das Problem ist, dass die ursprünglich geringe Wahrscheinlichkeit für das Auftreten solcher Fehler bei den heutigen Datenträgerkapazitäten plötzlich sehr groß werden. Die bei vielen Festplatten angegebene Wahrscheinlichkeit von einem URE pro 10^{14} Bytes entspricht 12 TB - selbst einzelne Datenträger erreichen heutzutage diese Kapazität.

Abhilfe können neuere RAID-Varianten schaffen, wie sie z.B. in ZFS-basierten Systemen eingesetzt werden. **RAIDz3** bietet mit 3 Redundanzen eine Sicherheitsstufe mehr als RAID-6 und bietet durch das zugrundeliegende Dateisystem ZFS weit höhere Absicherung gegen unentdeckte Fehler.

Noch sicherer ist z.B. **Erasure Coding**, ein Verfahren, das höhere Sicherheits-Konfigurationen erlaubt. Bei 4 Redundanzreserven ist der Ausfall eines Datenträgers unkritisch. Da der Rebuild mit moderatem Aufwand im Hintergrund erfolgen kann und Fehler beim Schreiben nahezu ausgeschlossen sind, eignet sich Erasure Coding gut zur Langzeitspeicherung.

Beim 12/8 Erasure Coding können bis zu 4 der 12 Datenträger ausfallen, ohne dass Datenverlust droht.
Werden je 4 Datenträger aus 3 unterschiedlichen Chargen eingesetzt, kann so auch der Ausfall einer kompletten Charge verkraftet werden.

Unabhängig vom Verfahren gibt es zusätzlich die Bedrohung des korrelierten Ausfalls von Datenträgern („**epidemic failure**“). Für Systeme, vor allem RAID-Konfigurationen, die den Einsatz vollständig gleicher Datenträger, möglichst aus derselben Charge mit exakt gleicher Firmware, erfordern, gilt: fällt ein Datenträger aus, sollte man die Daten so schnell wie möglich auf ein neues System umziehen. Je gleicher die Datenträger sind, desto ähnlicher verhalten sie sich bei gleicher Nutzung hinsichtlich der Ausfallwahrscheinlichkeit. Abhilfe sorgen hier Systeme, die den **Einsatz unterschiedlicher Datenträger** innerhalb des Redundanzverbundes ermöglichen. Durch den gezielten Einsatz unterschiedlicher Modelle oder Baureihen kann so der Ausfall einer kompletten Reihe verkraftet werden.

3. Die Zugriffs-Ebene

Die häufigste Ursache für Datenverlust ist immer noch: **der Mensch**. Dazu gehört zunehmend der kriminelle Mensch: das Thema **Ransomware** ist aktueller denn je. Dabei attackieren neue Varianten auch gezielt Backup-Daten, die im Netzwerk liegen. Verstärkt sind öffentliche Einrichtungen , vor allem Krankenhäuser, Ziele der Angriffe. Auch der klassische **Hackerangriff** ist präsenter denn je. Ein Email-Provider verlor kürzlich wahrscheinlich alle Emails und Backups der letzten 18 Jahre durch einen Hacker-Angriff.

t3n: Krankenhäuser werden immer häufiger Ziel von Hacker-Angriffen – https://t3n.de/news/krankenhaeuser-werden-immer-haeufiger-1139671/

Brian Krebs: Email Provider VFEmail Suffers ‘Catastrophic’ Hack – https://krebsonsecurity.com/2019/02/email-provider-vfemail-suffers-catastrophic-hack/

Es gilt also, den Zugriff auf Daten und Backups zu schützen. Die einhellige Meinung ist dabei jedoch, dass ein hundertprozentiger Schutz vor Angriffen zunehmend schwieriger, wenn nicht unmöglich ist. Auch wenn Firewalls, aktuelle Virenscanner und sonstige Zugriffsschutzmaßnahmen zum Standard gehören, müssen kritische Daten gesondert abgesichert werden. Dazu gehört auch, sich auf den Ernstfall, also den Ausfall der Primärspeicher, vorzubereiten. Verstärkt wird inzwischen (wieder) auf **offline-fähige Medien** gesetzt. Das Tape erlebt eine unerwartete Wiederbelebung. Die Sicherheit, bei Totalausfall des Online-Systems zumindest auf die letzte Sicherung, die offline und **zugriffssicher** verwahrt wird, zurückgreifen zu können, wiegt für viele die bekannten Nachteile der Tape-Systeme auf. Die reine Linearität und das komplizierte Handling von Tape-Systemen führt aber zu einem weiteren Problem: Die Hauptkosten bei einem Befall der IT durch Ransomware oder Hacking entstehen meist durch

FAST LTA
Wir sichern Petabytes.

die daraus resultierenden **Ausfallzeiten**, in denen ein Unternehmen nicht oder nur eingeschränkt operativ wirtschaften kann. So hatte der Logistik-Konzern Maersk mehrere hundert Millionen Dollar Verlust nach einer Attacke der Ransomware-Variante “NotPetya” zu verkraften.

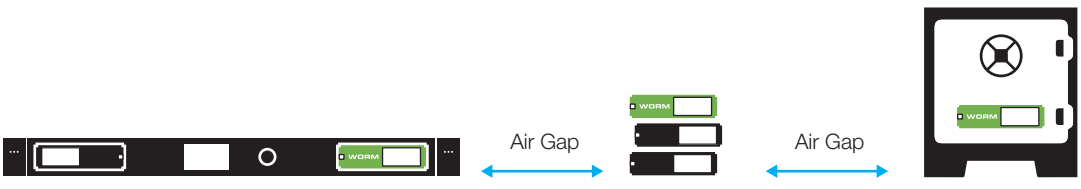
Forbes: NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million – https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/

Moderne Backup-Software bietet zur sofortigen Verfügbarkeit inzwischen die Möglichkeit, virtuelle Maschinen direkt vom Backup zu starten, während der Restore im Hintergrund läuft. Der laufende Betrieb kann so schnell wieder hergestellt werden, wenn auch mit reduzierter Performance. Wird zur Sicherung jedoch ein rein lineares Medium wie Tape eingesetzt, müssen die Daten dazu zuerst wieder auf ein System mit Random Access restauriert werden.

Benötigt werden also Lösungen, die einerseits die Möglichkeit des “**Air Gap**”, also der physischen Trennung von Speichermedien und Online-IT, als auch wahlfreien Zugriff und sofortige **Verfügbarkeit** der Daten ohne aufwändiges Kopieren bieten.

Um zusätzlich gegen **Manipulation** bereits gesicherter Daten geschützt zu sein, empfehlen sich Medien, die gegen Überschreiben und Löschen - absichtlich oder versehentlich - geschützt sind. Diese **WORM-Versiegelung** bietet dazu auch die in vielen Bereichen geforderte Rechtssicherheit durch **revisionssichere Archivierung**. Für die einfache Variante des “Soft(ware)-WORM” gilt aber dasselbe wie für jeden Zugriffsschutz: Wenn es eine Lücke in der Sicherheitskette gibt, kann die Versiegelung jederzeit aufgehoben und damit unbrauchbar gemacht werden. Wirklich sicher sind hier nur durch **Hardware-WORM** geschützte Medien, die Manipulation und ungewolltes Löschen zu 100% verhindern. Dass dies auch mit dem in der **EU-DSGVO** verankerten “Recht auf Löschung” vereinbar ist, zeigt z.B. ein kürzlich in Österreich gefälltes Urteil, nachdem Anonymisierung als Löschverfahren ausreicht. Ist ein Hardware-WORM-System zur revisionssicheren Archivierung zertifiziert, beinhaltet das auch die Möglichkeit, Daten unzugänglich machen zu können.

golem.de: Anonymisierung reicht als Löschverfahren aus – https://www.golem.de/news/dsgvo-beschwerde-anonymisierung-reicht-als-loeschverfahren-aus-1902-139334.html



Air Gap und Versiegelung durch Hardware-WORM schützen effektiv gegen unerlaubten Zugriff und ermöglichen es, rechtliche Grundlagen einzuhalten.

Fazit:

Datensicherung, Datensicherheit und Datenschutz

Zur sicheren Speicherung von Daten gehören neben **Einhaltung von Datenschutz** und **Maßnahmen zur Datensicherheit** auch die konsequente **Umsetzung der Datensicherung**. Zu bevorzugen sind Sekundärspeicher, die über eingebaute Mechanismen zur Datensicherung verfügen.

Lokale Unabhängigkeit durch **Replizierung**, Schutz vor Ausfall von Datenträgern durch **Redundanz**, und die Möglichkeit, den Zugriff auf Daten durch **Air Gap** und **Hardware-WORM** zu beschränken, sind die Hauptmerkmale eines sicheren Speichersystems, das alle 3 Ebenen der Datensicherung abdeckt.

Das Silent Brick System ist ein slot-basierter Sekundärspeicher. Jeder Silent Brick ist in verschiedenen Konfigurationen mit SSDs oder Festplatten mit optionaler Hardware-WORM Versiegelung verfügbar, lässt sich individuell konfigurieren und anbinden, und ist von Haus aus offline-fähig. Im selben System sind so separat skalierbare Bereiche für File Server, Archiv- und Backup-Speicher realisierbar.

Der Controller (im Bild) verfügt über 5 Slots und lässt sich durch Shelves mit je 14 Slots erweitern.

FAST LTA
Wir sichern Petabytes.

Design,
Entwicklung
und Support
in **Deutschland**

FAST LTA AG | Rüdesheimer Str. 11 | 80686 München | info@fast-lta.de | **www.fast-lta.de**