FAST LTA
Wir sichern Petabytes.

Faktencheck

Was kostet ein sicheres Backup?

Die Bedrohung durch Ransomware-Angriffe nimmt stetig zu. Weltweit geraten durch gezielte Angriffe ganze Handelsketten[1], Energieversorger[2] und IT-Dienstleister[3] in Schwierigkeiten. Da hinter vielen Attacken russische Hacker, evtl. mit Verbindungen zum russischen Geheimdienst, vermutet werden, führen Angriffe inzwischen zu politischen Spannungen[4]. Je nachdem, wie die Angreifer vorgehen, kann ein Ransomware-Angriff kaum verhindert werden.

Der Angriff der Gruppe REvil über das Desktop-Management-Tool Kaseya hat gezeigt, dass es im Grunde unmöglich ist, sich vor solchen Angriffen zu schützen, da der Schad-Code über eine eigentlich vertrauenswürdige Dritt-Software in die Systeme gelang. Bei der Strategie für ein „Ransomware-sicheres“ Backup-Konzept geht es also darum, den Regelbetrieb so schnell wie möglich wiederherzustellen. Es bleibt jedoch die wichtigste Frage: Was kostet mich so ein Backup?

1 https://www.heise.de/news/Hunderte-Coop-Supermaerkte-in-Schweden-nach-REvil-Ransomwarebefall-geschlossen-6128251.html

2 https://www.golem.de/news/ransomware-colonial-pipeline-ueber-kompromittiertes-passwort-gehackt-2106-157085.html

3 https://www.it-daily.net/shortnews/29385-revil-ransomware-angriff-ueber-msp-lieferkette-von-kaseya-vsa

4 https://www.reuters.com/technology/biden-says-uncertain-who-is-behind-latest-ransomware-attack-2021-07-03/

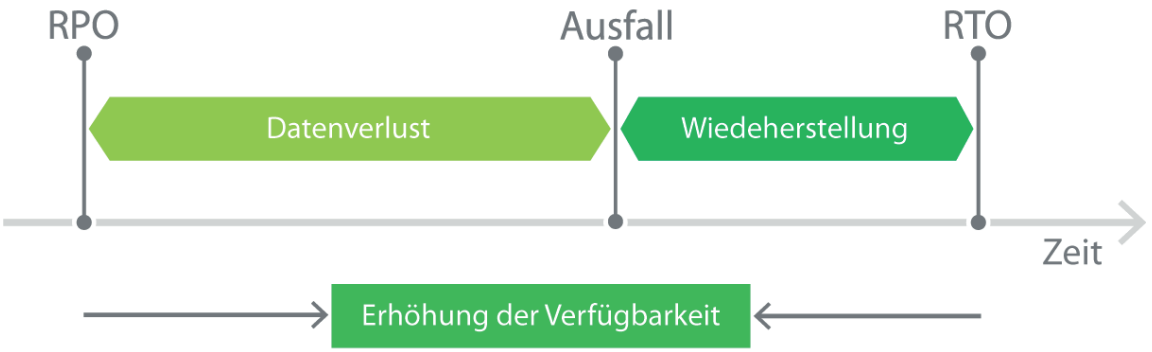
Stand: Juli 2021

Einflussfaktoren

Natürlich kann diese Frage nicht pauschal beantwortet werden. Zu viele Faktoren haben Einfluss auf die Kosten. Was man jedoch mit Sicherheit sagen kann: Vorausschauend zu handeln und in ein modernes Backup zu investieren, ist in jedem Fall günstiger, als sich nach einem erfolgten Angriff den immensen Folgekosten, von der Lösegeldzahlung bis zur aufwändigen Systemrettung, stellen zu müssen. Welche die fünf maßgeblichen Gründe für die ständig steigenden Folgekosten sind, haben wir im **Faktencheck „Was kostet ein Ransomware-Angriff“**[5] zusammengefasst. Je nach Angriff machen zwei Faktoren den Löwenanteil aus: Die eigentlichen Lösegeldforderungen werden immer höher, und die Folgekosten durch Ausfall der IT steigen mit jedem Tag. Es gilt also, eine Zahlung zu vermeiden und Zeitraum und Aufwand zur Wiederherstellung zu minimieren.

5 Download unter **https://fastlta.com/faktencheck-ransomware**

FAST LTA
Wir sichern Petabytes.



RPO & RTO - Quelle: Veeam

Faktor #1 – RPO & RTO

Entscheidend für die Minimierung der Ausfallzeit ist - neben dem Vorhandensein eines Backups - der so genannte RTO: Recovery Time Objective. Wie lange darf eine Wiederherstellung maximal dauern, ohne dass dem Unternehmen erheblicher Schaden entsteht? Der RTO hat natürlich für verschiedene Abteilungen oder Datenarten unterschiedliche Werte. Wenn Bestellungen nicht mehr einsehbar sind, das Flottenmanagement nicht verfügbar ist, oder schlicht die Kommunikation ausfällt, ist in der Regel höchste Eile geboten. Andere Daten müssen unter Umständen nicht unmittelbar wieder hergestellt werden. Der RTO hat entscheidenden Einfluss auf die geforderte Performance und die Größe der ersten Backup-Instanz, aus der Daten in kürzester Zeit wieder bereitgestellt werden müssen. Auch der RPO - Recovery Point Objective - spielt eine große Rolle, denn er bestimmt die Häufigkeit, mit der Full Backups bzw. Backups ganz allgemein erstellt werden müssen, und wie lange sie aufbewahrt werden sollen. Wie lange darf das letzte Backup zurückliegen - auch diese Frage ist sicher für verschiedene Anwendungen unterschiedlich zu beantworten.

Faktor #2 – Backups und Archive

Je größer ein Backup wird, je länger das Backup-Fenster wird, desto teurer und aufwändiger wird es. Es ist also sinnvoll, von vornherein zu identifizieren, welche und wie viele Daten überhaupt im Backup-Prozess sein müssen. Ein Backup ist immer eine Vervielfältigung von Daten. Nach der 3-2-1-Regel werden mindestens 3 Instanzen abgelegt, aber durch die zusätzliche Aufbewahrungszeit steigen die zu speichernden Datenmengen auf das bis zu 10-fache an. Ältere Backups, die der langfristigen Absicherung dienen, werden deshalb oft in so genannte Backup-Archive verschoben. Diese lagern auf günstigeren, sicheren Medien und reduzieren so die Kosten. Noch günstiger wird es, wenn man „kalte“ Daten, also solche, auf die nur noch sehr selten zugegriffen werden muss, auf einen Archivspeicher verschiebt. Moderne Archive haben nichts mehr mit dem digitalen Pendant der Keller voller Akten zu tun, wo Daten dem Tod entgegenschimmeln und im Grunde nur in Extremfällen abrufbar sind. Moderne Archive sind energiesparend, sicher und dabei jederzeit verfügbar. So lassen sich beispielsweise Big Data Analysen verwirklichen oder ältere Daten schnell auffinden. Da ein Archiv immer eine Verdrängung aus dem Arbeitsspeicher darstellt, fallen diese Daten aus dem Backup und reduzieren so die Datenmenge zum Teil erheblich.

René Weber, Field Application Engineer, erklärt auf unserem Youtube-Kanal unter **https://fastlta.com/youtube** die Unterschiede zwischen Backup und Archivierung

FAST LTA
Wir sichern Petabytes.

Bestandteile einer modernen Backup-Software - Quelle: Veeam

Faktor #3 – Infrastruktur und Software

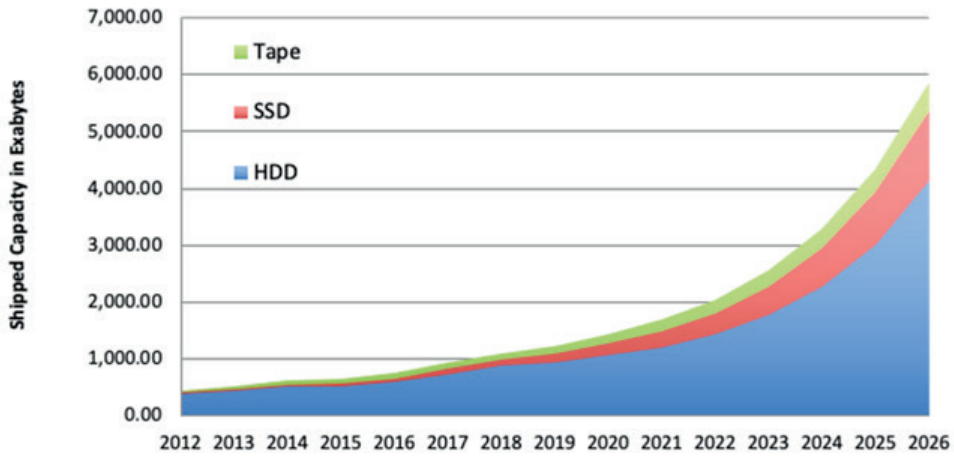
Kaum ein Unternehmen startet bei Null, wenn es um die Optimierung des Backups geht. Vorhandene Infrastruktur spielt eine entscheidende Rolle - auch in der Auswahl der entsprechenden Backup-Software. Komplett virtualisierte Umgebungen erfordern andere Konzepte als Unternehmen, die hauptsächlich mit großen Dateien umgehen müssen. Die Segmentierung der Abteilungen und Software-Lösungen - oft über Jahre „gewachsen“ - stellt eine weitere Hürde dar. Home Office und BYOD (Bring Your Own Device) verlangen nach Zero Trust Ansätzen zur Vermeidung von Einfallstoren für Schadsoftware.
Bei der Auswahl der Backup-Software gilt zudem, den Funktionsumfang gegen die eigenen Bedürfnisse abzuwägen und das Lizenzmodell dem aktuellen Stand, aber auch dem zu erwartenden Wachstum gemäß auszuwählen.

Faktor #4 – Die Datenmenge

Wie in #2 beschrieben, lässt sich die zu sichernde Datenmenge unter Umständen durch geschicktes Datenmanagement bereits vorab reduzieren. Dennoch bleiben die Größe eines vollständigen Backups und das zu erwartende Datenwachstum die entscheidenden Faktoren. Wichtig bei der Auswahl eines Backup-Speichers ist dabei, Wachstumsszenarien im Voraus zu evaluieren. Sehen Public Cloud Anbieter für kleinere Datenmenge zunächst wie eine scheinbar attraktive Lösung aus, stellen Kosten für den Abruf großer Datenmengen und die Limitierung der Verfügbarkeit eventuell später eine große Hürde dar. Einfache NAS-Systeme versprechen schnelle Lösungen bei geringer Investition, sind aber anfällig für Angriffe[6], nicht besonders sicher[7] und skalieren schlecht. Die notwendige Speicherkapazität teilt sich im Backup auf mehrere Bereiche gemäß der 3-2-1-Regel auf. Kurzfristig verfügbare Incrementals erfordern andere Speichertechnologien als langfristig sichere Backup-Archive oder transportfähige Air Gap Instanzen. Der Einsatz unterschiedlicher Technologien und zusätzlicher Sicherheitsmaßnahmen beeinflusst die Kosten für die Backup-Konfiguration maßgeblich.

6 https://www.kaspersky.de/blog/wd-my-book-remote-wipe/26976/

7 https://www.zdnet.com/article/why-raid-5-stops-working-in-2009/



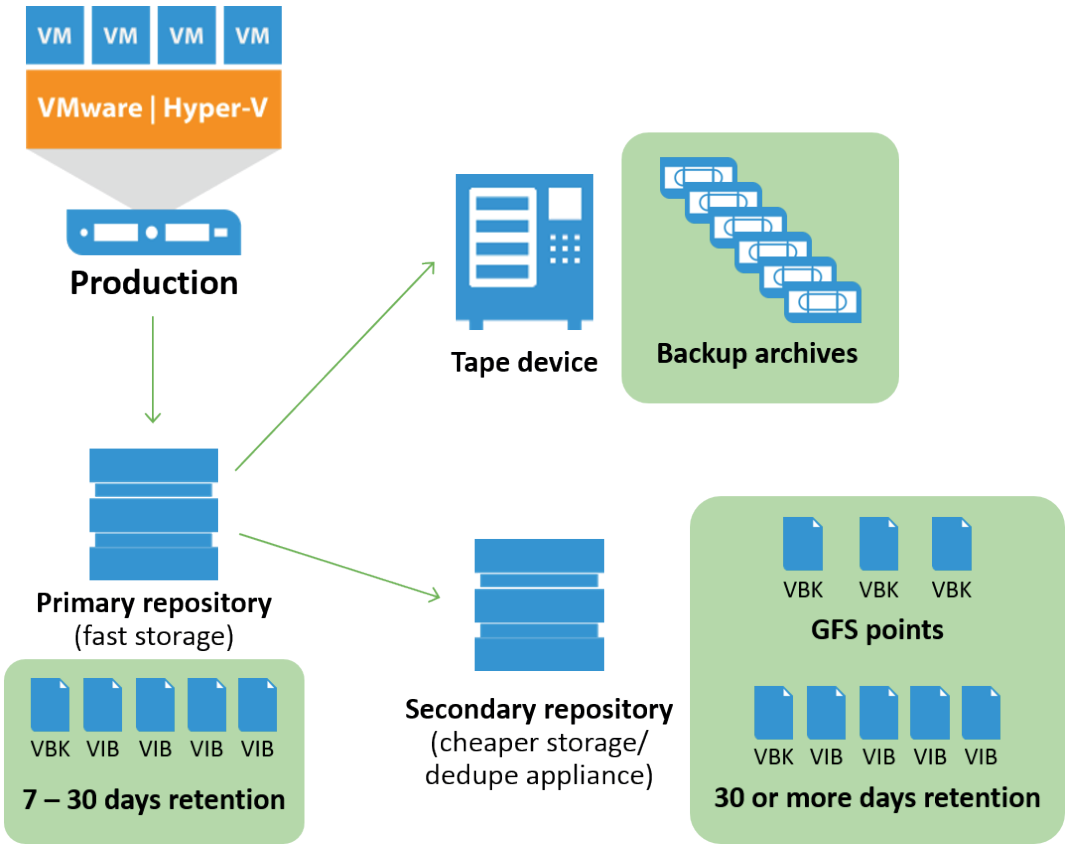
Festplatten werden auch in Zukunft den Großteil der benötigten Speicherkapazität abdecken - Quelle: Forbes

Beispiel-Konfigurationen

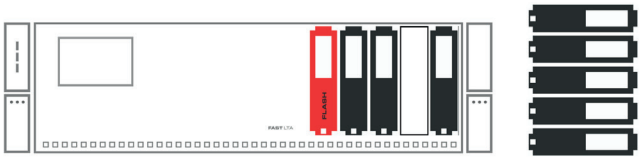
In den folgenden Beispielen haben wir uns an unseren **Veeam Mini-Guides**[8] orientiert. Wie oben beschrieben können die vorliegenden Konfigurationen nur einen Ausgangspunkt für die eigene Backup-Strategie darstellen. Zur Absicherung kommen dabei eine Reihe unterschiedlicher Technologien zum Einsatz, die in den Mini-Guides ausführlicher beschrieben sind. Besonders wichtig sind dabei die Continuous Snapshots, die zwar zusätzlichen Speicherplatz durch Sicherung der Änderungen kosten, es aber im Falle eines Ransomware-Angriffs erlauben, unkompliziert zur letzten unkompromittierten Version zurückzukehren. Zur Berechnung der benötigten Kapazität haben wir den Restore Point Simulator[9] genutzt. In den Preisangaben berücksichtigt sind Hardware-Kosten und Software-Lizenzen. Optionen, die u.U. zur Anbindung an die Netzwerk-Infrastruktur notwendig sind, Kosten für Replizierung, sowie der Wartungsvertrag sind nicht berücksichtigt.

8 Downmload unter **https://fastlta.com/veeam-de**

9 https://rps.dewin.me/



„Best Practice“ Backup-Strategie - Quelle: Veeam



Small – 4TB Daten: ab ~35.000€

Unsere Standard-Konfiguration geht von folgender Backup-Strategie aus:

- **Incrementals** mit täglicher Sicherung
  Intervall: 7 Tage.
  Benötigte Netto-Kapazität: ~7TB.
  Speichermedium: 1x Silent Brick Flash 12TB

- **Backup Copies** davon mit täglicher Sicherung
  Intervall: 4 Wochen, am Ende jeder Woche ein Full Backup (synthetisch, aus den Incrementals erzeugt), zusätzliche Absicherung durch Continuous Snapshots.
  Benötigte Nettokapazität: ~21TB.
  Speichermedien: 2x Silent Brick 24TB (oder 1x 24TB + 1x 12TB)

- **Air Gap** monatlich
  Aufbewahrung: 6 Monate, rotierend,
  entweder direkt aus dem Full Backup der Backup Copy (Clone) oder als VTL-Kopie durch die Backup-Software.
  Benötigte Nettokapazität pro Auslagerung: je nach Methode ~2 … 7TB.
  Speichermedien: 6x Silent Bricks 12TB

Als Basis-System dient ein Silent Brick Controller mit 5 Slots, da die ausgelagerten Silent Bricks keinen Slot belegen (und keine Lizenzen kosten).

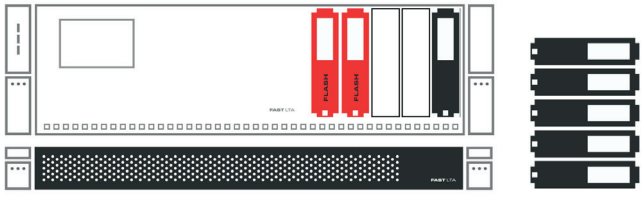
Medium – 20TB Daten: ab ~61.000€

Wird die Datenmenge im Vergleich zu Beispiel 1 verfünffacht, erkennt man deutlich die im Verhältnis günstigeren Speicherkosten - bei gleicher Konfiguration. Basis-Investments (Controller) sind nur einmal notwendig. Für die Backup Copies kommt der platz- und kostensparenden Silent Brick DS mit hoher Kapazität auf nur einer Höheneinheit zum Einsatz, da diese Daten üblicherweise nicht entnommen werden müssen. Dadurch reichen auch hier die 5 Slots eines Controllers aus. Zudem spart unser progressives Lizenzmodell bei steigender Datenmenge Kosten ein. Dies gilt auch für die nachträgliche Aufrüstung, bei der vorhandene Lizenzen gegen günstigere „eingetauscht“ werden.

- **Incrementals**: ~31TB auf 2x Silent Brick Flash 24TB

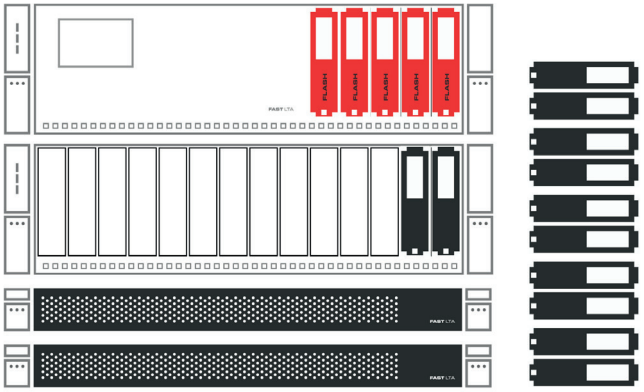
- **Backup Copies**: ~93TB auf Silent Brick DS 128TB

- **Air Gap**: je ~10TB auf 6x Silent Brick 24TB



FAST LTA
Wir sichern Petabytes.

FAST LTA
Wir sichern Petabytes.



Large – 60TB Daten: ab ~129.000€

Als Alternative zur Backup Copy bei großen Datenmengen bietet sich seit Veeam V10 der Capacity Tier an, der Daten auf einem S3 Object Store ablegt. Dabei wird durch die in Veeam dafür integrierte Deduplizierung Kapazität und Bandbreite gespart, was Kosten und Verfügbarkeit zugute kommt. Auch der Capacity Tier wird im Silent Brick System über Continuous Snapshot abgesichert. Statt einzelner Buckets wird so das gesamte S3-Volume direkt im Silent Brick System „immutable“. Die Sicherung via S3 erfordert keine zusätzliche Lizenz im Silent Brick System.

- **Incrementals**: ~83TB auf 5x Silent Brick Flash 24TB. Hier bietet sich alternativ auch ein Silent Brick DS mit 128TB als Speicher an, der allerdings nicht ganz die Performance der Silent Brick Flash erreicht.

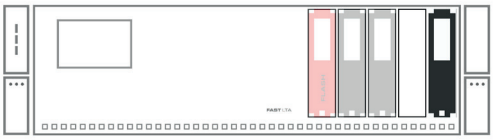
- **Capacity Tier** auf S3 On Premise Object Store mit Continuous Snapshots, fortlaufend
  Aufbewahrung: 4 Wochen
  Speicherbedarf: ~156TB
  Speichermedium: Silent Brick DS 192 TB.
  Neben der Option, Daten über den Capacity Tier zu kopieren, lassen sich ältere Daten auch auf dasselbe Medium verdrängen - und somit aus dem Backup-Fenster herausnehmen. Dies kann als Alternative oder Ergänzung zum Air Gap erfolgen.

- **Air Gap**: ~30TB auf 12x (6x je 2) Silent Brick 24TB

Silent Bricks sind Veeam-zertifizert

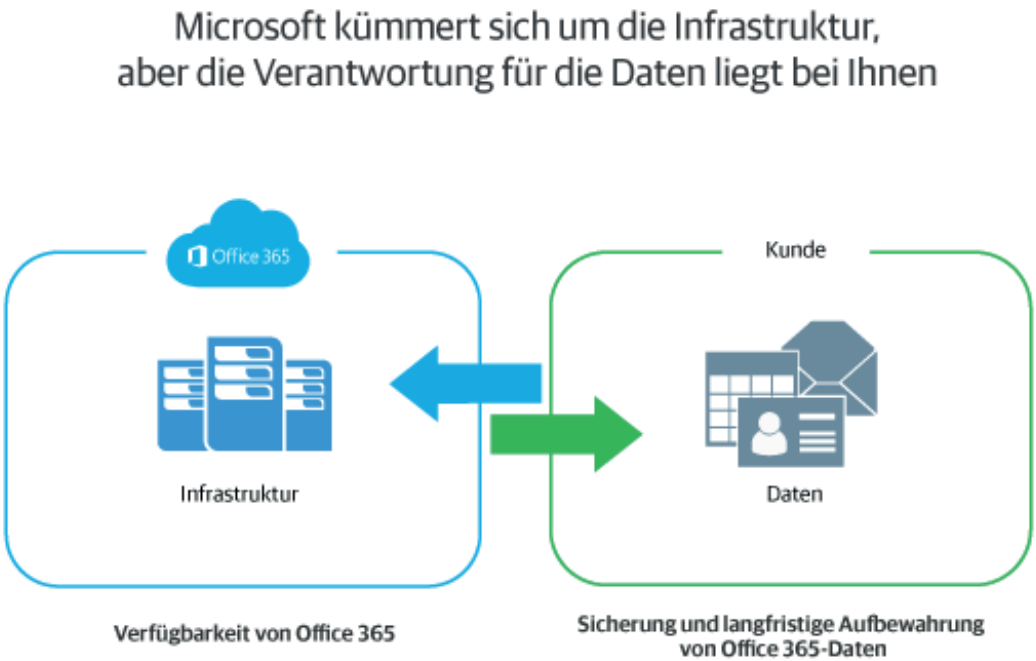
VEEAM READY Repository

Zusatz Office365-Backup – 6TB Daten: 1.000€



Das Backup Cloud-basierter Dienste wie Microsoft Office365 wird oft übersehen, ist jedoch ebenso wichtig wie die lokale Datensicherung. SaaS-Dienste kümmern sich zwar um den reibungslosen Betrieb, nicht jedoch um die Sicherung der Daten. Über Software-Pakete wie Veeam for Office365 lassen sich diese Daten im gleichen Setup einfach auf S3 Object Stores sichern. Die lokale Sicherung bringt dabei gegenüber einer Sicherung in der Public Cloud den Vorteil, dass im Fall eines Ransomware-Angriffs, wo als erste Maßnahme alle Verbindungen ins Internet gekappt werden müssen, die Daten dennoch lokal, sofort und ohne Zusatzkosten verfügbar sind.

- **Sicherung via S3** auf On Premise Object Store:
  ~6TB auf Silent Brick 12TB



Office365 - Quelle: Veeam

FAST LTA
Wir sichern Petabytes.

FAST LTA
Wir sichern Petabytes.

Zusatzoptionen

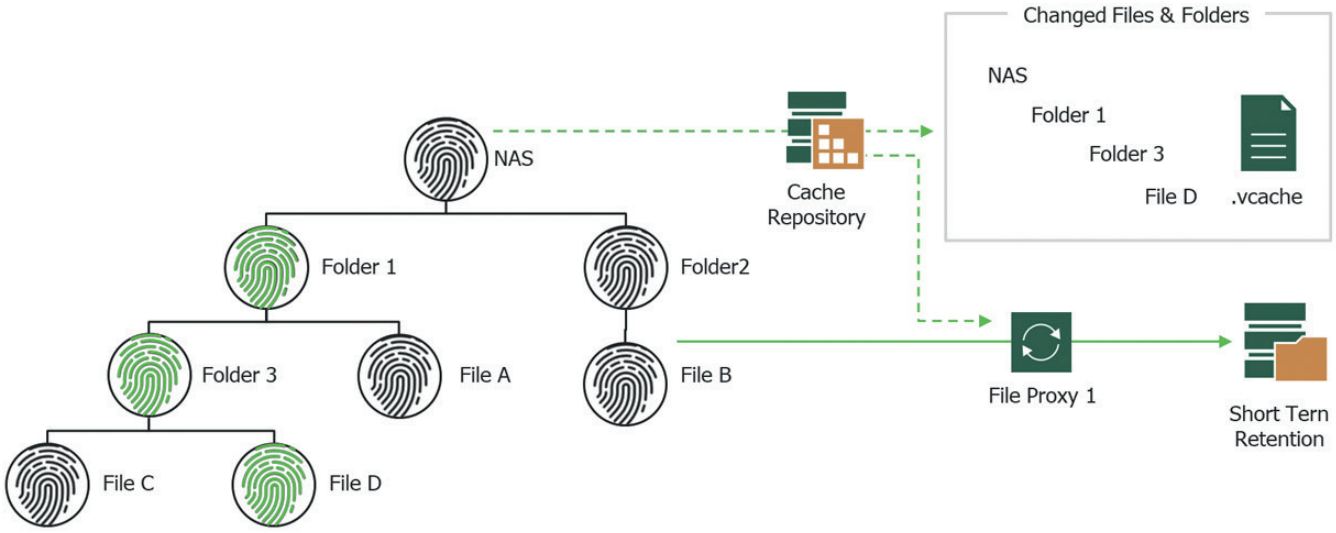
Neben dem oben kalkulierten klassischen 3-2-1-Backup für virtuelle Umgebungen sind im Zuge einer ganzheitlichen Datensicherung noch eine Reihe von weiteren Maßnahmen im Einzelfall zu evaluieren.

File Server Backup

Große, unstrukturierte Datenmengen liegen häufig auf (physischen) File Servern. Diese Daten ändern sich in der Regel nur inkrementell (es kommen hauptsächlich neue Daten hinzu), der Zugriff hält sich nach dem initialen Speichern meist in Grenzen. Ein klassisches Backup dieser Server würde den Prozess unnötig aufblähen und damit verlangsamen und verteuern. Veeam hat deshalb seit der Version 10 ein so genanntes NAS Backup integriert. Kerntechnologie ist das Changed File Tracking, das auf dem zu sichernden Server ständig die Änderungen im Dateisystem überwacht und nur veränderte bzw. neu hinzugekommene Daten sichert. Ein Full Backup ist deshalb nur einmalig am Anfang der Sicherung notwendig. Als Ziel dient erneut der S3 Object Store, als Medium bietet sich aufgrund der Kapazität der Silent Brick DS mit bis zu 192TB an.

Replizierung 1:n

Zur Absicherung gegen Komplettausfall, z. B. durch Brand, Wasserschaden oder Diebstahl, ist häufig eine Datenreplizierung zu einem zweiten Standort vorgeschrieben. Üblicherweise muss dazu ein komplettes System gespiegelt werden, was das Investment mehr oder weniger verdoppelt. Dabei müssen meist nicht alle Daten extra abgesichert werden. Im Silent Brick System erfolgt eine Replizierung nicht auf Systembasis sondern auf Grundlage einzelner Silent Bricks bzw. Volumes. Damit ist es problemlos möglich, z. B. nur Full Backups zu einem zweiten Standort zu replizieren, wo ein deutlich kleineres - günstigeres - System stehen kann. Auch die Replizierung über mehrere Standorte wird unterstützt, so dass sich beispielsweise Full Backups aus mehreren Filialen zentral sichern lassen.



Changed File Tracking - Quelle: Veeam

Weitere Anwendungen

Datensicherung umfasst nicht nur den Bereich Backup. Für die Ablage unstrukturierter Daten auf File Servern, die Nutzung eines aktiven Archivs oder auch die Notwendigkeit eines revisionssicheren und DSGVO-konformen Archivs haben sich Lösungen von FAST LTA seit Jahren in tausenden Installationen bewährt. Unsere Hardware-WORM-Technologie mit Erasure Coding und linearem Dateisystem schützt Daten zu 100% gegen Manipulation und unbeabsichtigtes Löschen. Da die Komplexität moderner IT und der damit verbundene Personal- und Wartungsaufwand eine der größten Herausforderungen darstellt, lassen sich durch Systemkonsolidierung im Sekundärdatenbereich weitere Einsparungen erzielen. Selbst wenn separate Systeme z. B. für Backup und Archivierung eingesetzt werden, profitieren Kunden von günstiger Gesamtlizenzierung und niedrigen Kosten / TB.

Wir erstellen Ihnen gerne ein individuelles Angebot.

Kontakt zum Vertrieb

Telefon: +49 (89) 890 47 610
Email: salesteam@fast-lta.de

FAST LTA
Wir sichern Petabytes.

Design,
Entwicklung
und Support
in **Deutschland**