FAST LTA
Wir sichern Terabytes.

COLD STORAGE

Erpressungs-Trojaner TeslaCrypt, Locky & Co

SICHERER SPEICHER: SCHUTZ VOR RANSOMWARE

Datum: März 2016
Autoren: Matthias Zahn
Hannes Heckel

Überblick

Im Gegensatz zu Zahlungs- oder Zugangsdaten hat ein persönlicher Datenbestand für Angreifer keinen Verkaufswert. Für den Eigentümer sind jedoch alle gespeicherten Informationen beliebig wertvoll.

Neue Computerviren zielen deshalb darauf, den Zugriff auf solche Daten durch Verschlüsselung zu verhindern und ein Lösegeld für die Freigabe zu erpressen.

Vollständiger Schutz vor solchen Angriffen wird zunehmend schwierig. Nur regelmäßige, „kalte“ Backups erlauben es, einen unbeschädigten Datenbestand wiederherzustellen.

Das richtige Storage kann diesen Prozess vereinfachen und Daten wirklich sicher gegen unautorisierte Verschlüsselung schützen.

Die Motivation für einen Angriff

Schadsoftware wird aus verschiedenen Motiven entwickelt und eingesetzt. Im Klassiker „War Games“ hackt sich ein Jugendlicher in die Kommandozentrale des US-Militärs und löst fast einen Weltkrieg aus - sicherlich aus heutiger Sicht kein realistisches Szenario.

Dennoch gibt es nach wie vor Hacker, die eigentlich keinen Schaden anrichten wollen und Hacking eher als Sport verstehen. Auch zur Sabotage, Überwachung und Spionage wird Schadsoftware entwickelt und verteilt - Stichwort: Bundestrojaner.

Wirtschaftliche Interessen

Den größten Anteil machen jedoch Angriffe aus wirtschaftlichen Interessen aus. Dabei ist es den Angreifern weitgehend egal, wen es trifft, so lange es eine Möglichkeit gibt, finanziellen Profit daraus schlagen zu können.

Lange Zeit war das so genannte Phishing am weitesten verbreitet. Das Absaugen von Kreditkarten- und Kontozugangsdaten stellt dabei eine unmittelbare, finanzielle Bedrohung dar.

Der Wert von Daten

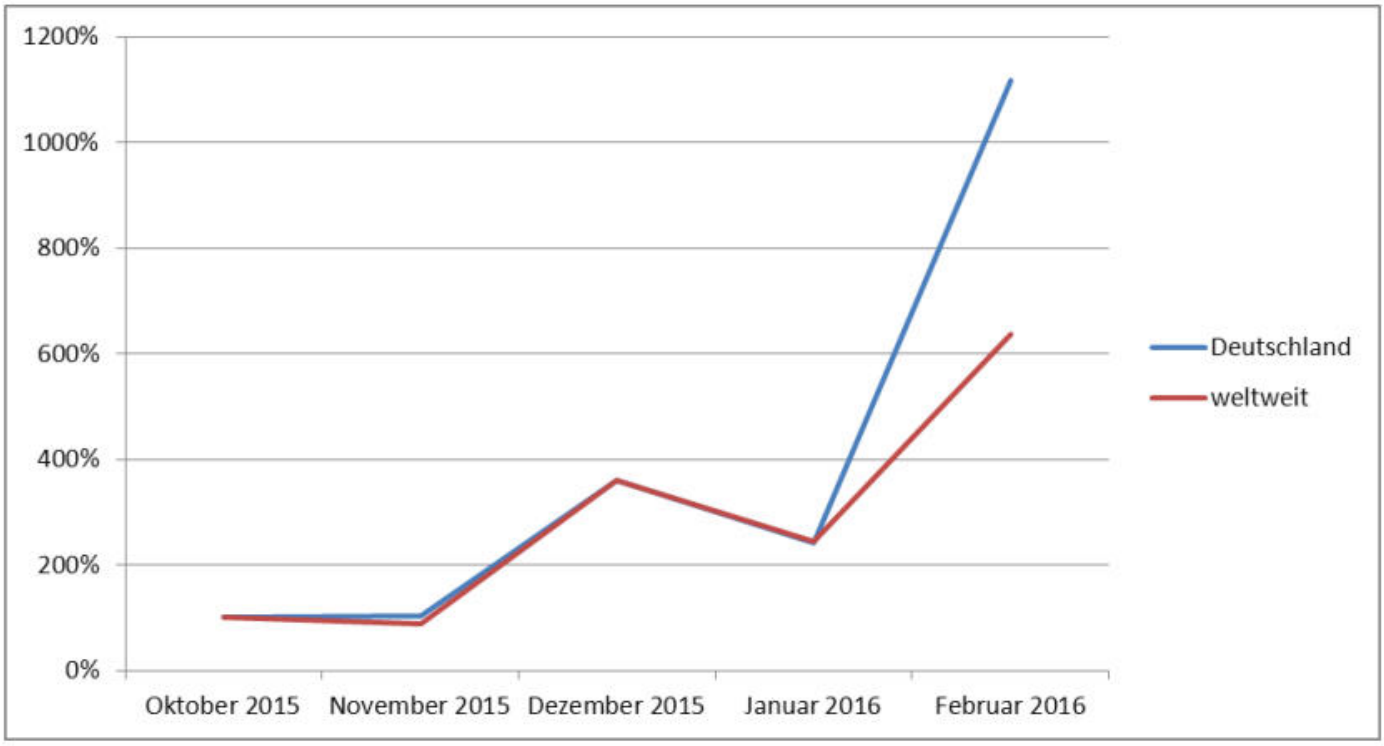
Diese Zugangsdaten haben also einen unmittelbaren **Marktwert**, Kreditkartendaten werden massenhaft im Darknet gehandelt. Da es sich bei Zugangs- und Kreditkartendaten aber um klar indentifizierbare Daten handelt, die im Vergleich zum Gesamtdatenbestand nur einen Bruchteil ausmachen, können diese mit vertretbarem Aufwand gut vor Missbrauch geschützt werden.

Der überwiegende Teil der auf Desktop-PCs, Servern und mobilen Geräten gespeicherten Daten hat für Angreifer keinen Wert - **sehr wohl jedoch für den Besitzer der Daten**.

Daraus entwickelt sich ein neues Geschäftsmodell: Erpressung.

> „**Anzeichen für Banking-Trojaner und DDoS-Angriffsclients werden auf den Clients teilweise ignoriert bzw. nicht aktiv verfolgt. Genauso werden häufig Fehlkonfigurationen von Systemen vernachlässigt, da diese keine Auswirkung auf den Wirkbetrieb haben. Die Schäden im Unternehmen sind in diesen Fällen nur gering. Die Schutzgelderpressung führt nun zu konkreten**

Schäden, bei denen man nicht mehr "wegschauen" kann“, so das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer aktuellen Studie.[1]



Von Oktober bis Februar hat sich die Zahl der Ransomware-Detektionen in Deutschland mehr als verzehnfacht - Quelle: BSI

Ransomware

Ransomware (engl.: ransom = Lösegeld) nutzt dieses Prinzip der Erpressung aus. Es gibt zwei Arten von Ransomware: Lockout und Crypto. Lockout sperrt den Zugang zum gesamten System und gibt ihn erst nach Zahlung einer „Gebühr“ wieder frei. In den meisten Fällen wird behauptet, dass „offizielle“ Behörden (FBI, Bundespolizei) den Zugang aufgrund illegaler Tätigkeiten sperren (Kinderpornographie, illegale Downloads, etc.).

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf;jsessionid=7E0D530953F100C88EB212938BE1DC4A.2_cid294?__blob=publicationFile&v=2

Am stärksten wachsend sind jedoch die Angriffe durch Crypto-Trojaner. Diese Schadsoftware verschlüsselt Teile der auf dem PC, Server oder mobilen Gerät gespeicherten Daten, so dass ein Zugriff darauf nicht mehr möglich ist. Die Hauptfunktionen des PCs bleiben erhalten, so dass der Schaden oft erst spät entdeckt wird - und der PC weiterhin operabel ist, z.B. um eine Zahlung auszulösen.

Die eingesetzte Verschlüsselung wird dabei ständig verbessert und neuesten Erkenntnissen angepasst - und ist damit selbst von Experten derzeit nicht zu knacken[2].

Zielgruppe: 100%

Wie oben beschrieben, vergrößert sich die Zielgruppe für derartige Angriffe auf nahezu 100% aller möglichen Ziele, da die gespeicherten Daten für den Besitzer beliebig wertvoll sind, auch wenn sie für andere so gut wie keinen Wert darstellen.

Für die Angreifer ist es dabei relativ egal, wen sie erwischen. Privatpersonen hängen sehr an persönlichen Erinnerungen (Fotos, Videos, Aufzeichnungen), für Unternehmen sind bestimmte Daten oft überlebenswichtig, und öffentliche Einrichtungen können ohne entsprechende Daten oft tagelang nicht oder nur eingeschränkt operieren.

Problem Geldübergabe: gelöst

Eine weitere Entwicklung spielt dabei den Angreifern in die Hände. Anonymer Zahlungsverkehr ist durch die Einführung von Crypto-Währungen wie Bitcoins sehr viel einfacher geworden. Es ist so gut wie unmöglich, diese Zahlungen nachzuverfolgen und den Empfänger ausfindig zu machen.

Durch diese beiden Rahmenbedingungen ändert sich die Situation für Schadsoftware entscheidend. Dass Betriebssysteme über mehrere tausend Schwachstellen pro Jahr angreifbar sind, ist nicht neu - dass damit sofort und bei jedem erheblicher Schaden mit finanziellen Konsequenzen droht, schon.

[2] http://www.engadget.com/2016/03/17/teslacrypt-can-no-longer-be-cracked/

Gegenmaßnahmen

Der erste Instinkt, ist, den Zugang zu sichern. Wird verhindert, dass sich ein Virus auf dem PC einnistet, kann er auch keinen Schaden anrichten. Aktuelle Virenscanner, regelmäßige Sicherheits-Updates, restriktive Firewalls, sowie eingeschränkte Nutzerrechte im Normalbetrieb gehören zu den unbedingt notwendigen Maßnahmen.

Dennoch wird es immer eine Schwachstelle geben, die keine Firewall schließen kann: den Menschen.

Beispiel: NSA

Die IT der NSA gehört sicher zu den am besten gesicherten der Welt. Dennoch konnte ein Berater, sein Name ist Edward Snowden, tausende brisante und als geheim eingestufte Dokumente aus dem System abziehen. Kein Virenscanner schlägt hier Alarm.

Und wenn einzelne Menschen Zugriff auf kritische IT-Bereiche haben können - und das müssen sie, schließlich muss man ja an die Daten kommen, um mit ihnen arbeiten zu können - können über diese Schwachstellen auch Viren ins System gelangen.

Die Problematik verstärkt sich zunehmend durch eine weitere Entwicklung: BYOD. „Bring Your Own Device“ ist die eingebaute Hintertür in fast jedes Unternehmen, jede Organisation. Mitarbeiter nehmen Laptops mit nach Hause, bringen ihre Smart Phones und Tablets mit in die Arbeit, oder greifen über Cloud Services und VPNs auf Daten und Firmennetzwerke zu. Ein vollständiges Aussperren dieser Fremdzugriffe ist in den meisten Fällen nicht möglich - und oft auch gar nicht gewünscht. Wie sonst sollen Vertriebsmitarbeiter im Außendienst arbeiten, und auch Outsourcing und Home Office wären nicht möglich.

Kalte Backups

Weil der Zugang zu Daten also kaum zu 100% abgedichtet werden kann, rät man zusätzlich dazu, „kalte“ Backups zu erstellen.

Als „kalt“ werden Medien bezeichnet, die keine Möglichkeit des Überschreibens zulassen - sei es, weil diese Medien offline gelagert werden, oder weil sie prinzipbedingt nur einmalig beschrieben werden können (WORM - Write Once Read Many). Daten auf diesen Datenträgern sind also vor Angriffen geschützt.

Dabei muss natürlich sichergestellt werden, dass sowohl der Prozess des Backups selbst als auch die Wiederherstellung in jeweils „sauberen“ Systemen geschehen.

Eine unterschätzte Gefahr geht dabei von den so genannten Metadaten aus. Die meisten Dateisysteme, auch die von Backup-Medien, vertrauen auf einen zentralen Index zur Identifikation der Nutzdaten auf dem Datenträger. Diese eigene Partition enthält alle Informationen, die notwendig sind, um aus den auf dem Datenträger fragmentiert gespeicherten Datenpaketen die ursprünglichen Dateien wieder herzustellen. Für einen Angreifer reicht es also, etwa bei automatisierten Backup-Prozessen, diesen Index zu infizieren, um eine Wiederherstellung unmöglich zu machen - auch wenn das Backup anscheinend intakt ist.

Das FBI warnt inzwischen explizit davor, dass neue Viren ganz gezielt nach Netzwerk-Backups suchen und diese löschen bzw. unzugänglich machen[3]. Was auch logisch ist - schließlich sind Netzwerk-Backups alles andere als „kalt“, da mit dem operativen System verbunden.

Und obwohl Netzwerk- oder Disk-to-Disk-Backups üblicherweise zusätzlich über (kalte) Magnetbänder abgesichert werden, kann so ein Angriff, je nach Zeitplan der Sicherungen, zum Verlust wertvoller Daten führen.

Trend: Ständige Verfügbarkeit aller Daten

Kalte Backups kommen allerdings gerade aus der Mode, da alle Daten möglichst ständig und sofort verfügbar sein sollen. Auswertungen via „Big Data“-Analysen, die Notwendigkeit der „Business Continuity“ im Fehlerfall, und die Kapazitätssprünge bei schnellen, verfügbaren Festplattenspeichern sehen ein „kaltes“ Backup in den meisten Fällen nur noch als allerletzte Sicherung vor. Die Wiederherstellung von Daten aus diesen Backups ist umständlich und im Vergleich langsam.

Teile der verfügbaren Speichersysteme, auf denen Daten vielfach gespiegelt und horizontal über viele Datenträger verteilt gespeichert sind, werden deshalb oft als „WORM“ deklariert. Dies geschieht, vereinfacht gesagt, über einen Schalter, der dem Dateisystem das Medium als „read only“ meldet. Dieses „Software-WORM“ wird zurecht als „Soft-WORM“ bezeichnet, da es lediglich auf Basis von Admin-Rechten abgesichert ist. Denn obwohl dieses Umschalten nur von Benutzern mit Admin-Rechten möglich ist, gilt auch hier erneut die oben aufgestellte Regel: Was „gute“ Menschen tun können, wird auch „bösen“ Menschen oder Algorithmen gelingen. Oft haben auch zu viele Benutzer Admin-Rechte im Netzwerk, was die Möglichkeit eines Angriffs vereinfacht.

[3] http://eweb.cabq.gov/CyberSecurity/Security%20Related%20Documents/FLASH%20MC-000068-MW.pdf

Sichere Speicherung

Wie muss also ein Speichersystem aussehen, das den aktuellen Anforderungen genügt und dennoch sicher ist?

Struktursicherheit

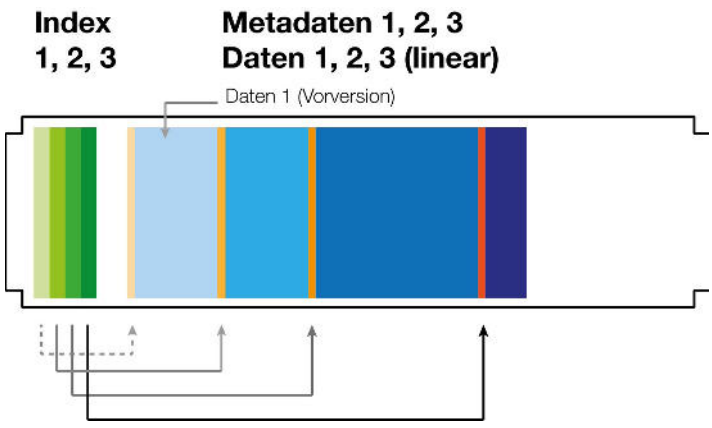
Die Voraussetzung für eine sichere Speicherung ist die Struktursicherheit, d.h. die Unabhängigkeit der Nutzdaten von einem zentralen Index oder Metadaten.

Allerdings ist die Umsetzung dieser Anforderung mit herkömmlichen Speichermethoden und Dateisystemen eher nicht vereinbar. Festplatten- oder Flash-Systeme legen Daten fragmentiert mit einem zentralen Index ab, da nur so die notwendige Geschwindigkeit und Lebensdauer sichergestellt werden kann. Ein „Löschen“ von Daten führt dazu, dass die entsprechenden Speicherbereiche im Index als „frei“ markiert werden und somit wieder überschrieben werden können. Die Nutzdaten selbst sind so lange noch auf dem Speicher vorhanden, ein Zugriff darauf ist aber in der Regel nicht mehr möglich. Dies gilt vor allem bei komplexen Speichersystemen mit vielen Redundanzen (Schutz durch RAID oder andere Mechanismen), die Daten ganz bewusst über viele Datenträger verteilt speichern. Während bei einer versehentlich „gelöschten“ SD-Karte also Daten noch relativ einfach wiederhergestellt werden können, ist das in komplexen Umgebungen nicht möglich.

Eine **struktursichere Speicherung** sieht dagegen vor, dass die zugehörigen Metadaten stets zusammen mit den Nutzdaten abgelegt werden. Um die Zugriffe zu minimieren und die Geschwindigkeit zu erhöhen, wird im Normalfall der zentrale Index verwendet. Eine Wiederherstellung ohne diesen Index ist aber eben auch direkt aus den Nutzdaten möglich.

Lineare Speicherung

Struktursicherheit funktioniert aber nicht mit verteilter Speicherung und Fragmentierung, da sonst bei jedem Datenfragment der gesamte Meta-Datensatz mit gespeichert sein müsste. Zudem werden beim „Random Write“ ja frei gewordene Speicherbereiche früher oder später wieder überschrieben, eine Wiederherstellung „gelöschter“ Daten ist also nur bedingt denkbar.



Abhilfe schafft hier eine **lineare Speicherung**. Wie auf Magnetband werden dabei zusammengehörende Datenpakete auch physikalisch zusammen hintereinander

abgelegt. Neue Daten werden stets am Ende des Datenbestandes angehängt - egal, ob durch „Löschen“ eigentlich weiter „vorne“ auf dem Medium wieder freie Bereiche existieren. Erst eine so genannte „Garbage Collection“ kompaktiert die Daten so, dass freie Bereiche keine Lücken mehr hinterlassen.

Diesen Umstand kann man sich zunutze machen, indem man die automatische Garbage Collection abschafft. Damit wird auf dem Speichermedium zwar mehr Speicherplatz verbraucht, Vorversionen sind jedoch jederzeit verfügbar, auch wenn sie nicht mehr im zentralen Index gespeichert sind - oder dieser manipuliert wird. In Kombination mit der Strukturicherheit ist ein „Zurückgehen“ auf solche Vorversionen also mit wenig Aufwand möglich.

Nutzt man nun moderne Redundanzmethoden wie Erasure Resilient Coding (auch kurz Erasure Code oder ERC genannt), ist dieses Prinzip auch auf hochredundanten Festplattensystemen realisierbar, die den gewohnt schnellen und wahlfreien Zugriff auf alle gespeicherten Daten bieten.

Auf so einem System muss nun ein Angreifer explizit den gesamten Datenträger überschreiben, um den Zugriff auf die gespeicherten Daten zu verhindern. Ein normales „Löschen“, was ja nur den zentralen Index verändert, erzeugt keinen Schaden. Eine Verschlüsselung würde ebenfalls nur eine neue Version der Daten auf dem Datenträger ablegen, die intakte Vorversion aber unberührt lassen.

Niemand darf Daten manipulieren können

Die struktursichere Speicherung ist die Voraussetzung dafür, dass Daten wiederhergestellt werden können, auch wenn zentraler Index oder Dateisystem korrupt oder manipuliert sind.

Der entscheidende Schritt zu einem wirklich sicheren Speichersystem ist aber die oben angesprochene „kalte Speicherung“, also der Schutz vor Manipulation, Löschen und Überschreiben. Dieser Schutz erfordert eine Entkoppelung des Speichers von allen Software-Zugriffen.

Gibt es auch nur eine Hintertür, kann diese über kurz oder lang auch ausgenutzt werden. Dies ist der Grund, wieso sich Apple so vehement gegen die Forderung des FBI nach einer Hintertür zu seinem mobilen iOS-Betriebssystem wehrt.

Ein anderes Beispiel sind die Sicherheitsschlüssel der Flughafenbehörden, mit denen die „Transport Security Administration“ (TSA) Koffer am Flughafen öffnen kann,

ohne Schlösser aufbrechen zu müssen. Es gibt 6 solcher Generalschlüssel, die Schlösser an Koffern tragen so genannte TSA-Codes, die den jeweiligen Schlüssel markieren. Irgendwann tauchte ein hochauflösendes Foto aller dieser Schlüssel auf. Seitdem kann jeder per 3D-Druck diese Schlüssel nachmachen - und damit theoretisch jeden Koffer gewaltfrei öffnen[4].

Diese Fälle zeigen: Wo es eine Möglichkeit zur Umgehung von Schutzmaßnahmen gibt, wird diese auch genutzt.

Das sichere Speichersystem muss also als oberste Prämisse haben: **Niemand darf die Möglichkeit haben, Daten zu überschreiben.**

Dazu gibt es zwei Möglichkeiten: Daten physisch aus dem laufenden System entfernen, oder gespeicherte Daten per Hardware-Schutz so zu „versiegeln“, dass ein Überschreiben nicht möglich ist, ohne den gesamten Speicher zu zerstören - was einer Erpressung die Grundlage entziehen würde.

Offline-Fähigkeit mit Replikation

Am einfachsten ist ein Zugriff auf Daten dadurch zu verhindern, dass Daten keine physische Verbindung zum laufenden System haben, also auf Medien gespeichert sind, die offline, z.B. in einem Safe, gelagert werden. Das funktioniert gut mit Daten, die nicht mehr benötigt werden. Daten, die weiterhin verfügbar sein sollen, werden vorher auf ein kaltes Medium repliziert und dann aus dem System entfernt. Ist der Replikationsprozess regelmäßig und häufig genug, gehen im Ernstfall keine oder kaum Daten verloren.

Offline-Medien eignen sich aber meist nicht dazu, im Ernstfall Daten sofort wieder verfügbar zu machen, wenn das Primärmedium kompromittiert wurde. Die Daten müssen erst umständlich vom Offline-Medium wieder hergestellt werden. Dieser Prozess ist zeitaufwändig - und auch fehleranfällig.

Das sichere Speichersystem muss also direkt auf offline-fähige Medien speichern, die sich bei Bedarf replizieren und aus dem System entnehmen lassen. Sollte ein Primärmedium befallen sein, wird die letzte Replika einfach im (dann hoffentlich „sauberen“) System gemountet, die Daten stehen sofort und ohne Wiederherstellen wieder zur Verfügung.

Da übliche Speichersysteme auf hochgradig verteilter Speicherung und Fragmentierung basieren, ist das nur mit der oben beschriebenen linearen Speicherung möglich. In Verbindung mit Erasure Coding sind so trotz hoher Sicherheit durch Redundanz und hoher Geschwindigkeit dank Datenträger-Verbund echte Offline-Medien realisierbar.

---

[4] http://www.heise.de/make/meldung/Hack-mit-3D-Drucker-TSA-Generalschluessel-fuer-Gepaeck-2810177.html

WORM-Versiegelung

Ein Überschreiben von Daten kann auch über eine **WORM-Versiegelung** verhindert werden. Die Datenträger müssen dabei nicht physisch aus dem laufenden Betrieb entfernt werden. Wie oben beschrieben ist die übliche „Soft-WORM"-Methode jedoch ebenfalls angreifbar und somit unsicher. Abhilfe schafft hier ein Hardware-Controller, der bei den angeschlossenen Datenträgern ein Zurücksetzen der Marke des letzten Schreibens verhindert. Ein physikalisches Überschreiben per Software ist damit unmöglich. Auch dies ist nur mit linearer Speicherung möglich, da sich die Medien gleichmäßig und ansteigend „auffüllen" und Daten nicht fragmentiert abgelegt werden.

Um auch diesen Sicherheitsaspekt auszuhebeln, müsste ein Angreifer die Funktionalität des speziellen Festplatten-Controllers mit der zusätzlichen Möglichkeit des Überschreibens nachbauen, die Festplatten physikalisch auf den neuen Controller „umhängen" und dann die unverschlüsselten Vorgängerversionen überschreiben.

Nutzung

Die oben beschriebenen Maßnahmen eignen sich nicht für jedes Speichersystem. Wenn Daten sehr oft verändert werden, wie das zum Beispiel bei Datenbanken der Fall ist, würde so ein Speichersystem schnell „voll laufen" - und damit nicht wirtschaftlich sein. Solche Systeme müssen weiterhin über regelmäßige Backups gesichert werden.

Gut geeignet ist ein solcher „kalter Speicher" jedoch für Daten, die sich in der Regel nach dem Schreiben nicht mehr ändern (sollen). Backups, Mediendaten (Fotos, Videos), aber auch Archivdaten (abgeschlossene Projekte, Studien, Messdaten, Überwachungsdaten, usw.) erfüllen diese Voraussetzungen.

Muss zudem bewiesen werden können, dass einmal geschriebene Daten nicht manipuliert wurden, spricht man von revisionssicherer Speicherung.

Speichersysteme von FAST LTA

FAST LTA hat mit **Silent Cubes** und **Silent Bricks** zwei Speichersysteme entwickelt, die mit linearer Speicherung mit Struktursicherheit, modernem Erasure Coding mit 4 Redundanzen, und weiteren Sicherheitsaspekten für kalte Speicherung, „Cold Storage“, optimiert sind.

Dreifache Absicherung gegen Datenverlust

Neben der hohen eingebauten Sicherung durch lineare Speicherung und Struktursicherheit verfügen Speichersysteme von FAST LTA über einen dreifachen Schutz vor Datenverlust durch Festplattenausfall.

Erasure Coding

FAST LTA setzt ein 12/8 Erasure Coding ein. Jede Speichereinheit verfügt über 12 Datenträger, von denen bis zu 4 gleichzeitig ausfallen können, ohne dass Daten verloren gehen. Ein entscheidender Vorteil gegenüber RAID-Konfigurationen ist dabei neben der höheren Sicherheit und dem besseren Brutto-/Netto-Verhältnis der deutlich reduzierte Aufwand für einen Rebuild.

> **“Mit Festplatten der heutigen Größe brauchen Festplatten-Arrays mit RAID für einen Festplatten-Rebuild Wochen, mit Erasure Coding ist das in wenigen Stunden erledigt”**, sagt zum Beispiel George Crump, Präsident des IT-Analysten Storage Switzerland.[5]

Dies ist zudem ein nicht zu unterschätzender Sicherheitsaspekt. Während eines Festplatten-Rebuilds befindet sich ein RAID-System in einem kritischen Zustand, ein weiterer Festplattenausfall hat dann oft schon Datenverlust zur Folge. Erasure Coding mit 4 Redundanzen hat beim Ausfall einer Festplatte noch 3 weitere Reserven, so dass der Rebuild, der sowieso viel weniger aufwändiger ist, entspannt und mit wenig Systemlast erfolgen kann.

Digital Audit

Das wichtigste am Backup ist, dass der Restore funktioniert. Diese Binsenweisheit setzt voraus, dass die gespeicherten Daten auch sicher wieder lesbar sind. Deswegen werden die Datenträger in Speicherprodukten von FAST LTA regelmäßig auf Bitlevel überprüft - der so genannte Digital Audit. Fehler werden so sicher erkannt und können behoben werden.

---

[5] Quelle: Search Storage, http://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2016

Disk Mix

Immer wieder kommt es vor, dass eine ganze Charge von Festplatten von einem Fehler betroffen ist. Aber auch im Normalbetrieb fallen Modelle aus der gleichen Charge oft in kurzen Zeitabständen aus.

Um dem vorzubeugen werde in jeder Speichereinheit Festplatten aus 3 verschiedenen Chargen von möglichst verschiedenen Herstellern[6] eingesetzt. Selbst wenn die 4 Festplatten der gesamten Charge ausfallen, gehen durch das 12/8 Erasure Coding in Silent Cubes und Silent Bricks keine Daten verloren.

Die Unabhängigkeit von bestimmten Datenträgertypen und Herstellern bietet zudem den Vorteil der Wahlfreiheit beim Ersatz. Auch nach Jahren ist ein Tausch einzelner Datenträger problemlos möglich.

Silent Cubes: revisionssicherer Archivspeicher mit WORM-Versiegelung

Der **Silent Cube** schützt Daten zusätzlich über eine WORM-Versiegelung vor Verlust. Da diese Versiegelung auf unterster Hardware-Ebene realisiert ist - der eigens entwickelte Festplattencontroller kann nur fortlaufend schreiben, aber weder löschen noch weiter vorne überschreiben - kann kein Admin, auch nicht FAST LTA, Daten verändern oder löschen.

Diese Funktionalität verleiht dem Silent Cube auch die Revisionssicherheit, die für Deutschland, Österreich und die Schweiz eine rechtskonforme Archivierung z.B. nach RöV, GoBS, GDPdU, ermöglicht.

[6] Leider gibt es für manche Festplattengrößen und SSD-Modelle gar keine 3 Hersteller mehr.

Silent Brick Library: Flexibles und sicheres Speichersystem für Backup und Archiv mit offline-fähigen Speicher-Containern

Die **Silent Brick Library** zielt auf einen weniger speziellen Markt. Als Cold Storage ist sie ideal als Ziel für Backups, aber auch als aktives Archiv, sowie als Netzwerkspeicher geeignet.

Die Basis bilden die **Silent Bricks**, offline-fähige Speicher-Container mit jeweils 12 Festplatten, die über das Erasure Coding in sich geschützt sind. Über die flexible Replikation auf Basis einzelner Silent Bricks lassen sich Offline-Kopien und Replikas an einem zweiten Standort besonders einfach und günstig erstellen. Anders als bei der üblichen Absicherung durch Spiegelung ann die Replizierung für jedes Medium individuell konfiguriert werden. Das zweite System bleibt dabei am zweiten Standort vollständig einsetzbar und kann seinerseits Silent Bricks in das erste System replizieren (Über-Kreuz-Replizierung).

Der Controller verfügt über 5 Slots für Silent Bricks und kann über direkt angeschlossene Erweiterungs-Einheiten mit je 14 Slots, sowie über per Netzwerk verbundene Silent Brick Drives mit 2 Slots erweitert werden.

Ein Silent Brick Drive ist durch die 2 Slots bereits ein idealer Speicher für kleine Speicheraufgaben, wie z.B. sichere Netzwerk-Backups mit der Möglichkeit der internen Replizierung auf den zweiten Silent Brick.

FAST LTA
Wir sichern Terabytes.

Über FAST LTA

Leidenschaft für Datensicherung

Wir sichern Terabytes - das ist der Leitsatz der FAST LTA AG, München. Im Slogan steckt das Versprechen, sich um die Daten der Kunden zu kümmern. Und das spiegelt sich in jedem Detail der von Matthias Zahn und seinen Mitarbeitern entwickelten Speicherprodukte wieder.

Der eigene Anspruch: Es dürfen keine Daten verloren gehen. Deswegen werden alle kritischen Komponenten selbst entwickelt, ausgiebig getestet, und ständig verbessert. Dazu gehört die Implementierung des Erasure Codings, eine dem herkömmlichen RAID überlegene Redundanzkodierung zum Schutz gegen Datenverlust. Diese Technologie ergänzt FAST LTA durch die Selbstüberprüfung namens Digital Audit und sichert jeden Redundanzverbund zusätzlich via Disk Mix ab, den Einsatz von drei verschiedenen Festplattenmodellen innerhalb einer Speichereinheit. Speicherprodukte von FAST LTA sind so sicher, dass - Sicherheit des Standortes vorausgesetzt - keine weitere Absicherung durch ein Backup notwendig ist.

Silent Cubes, der revisionssichere WORM-Speicher für alle Daten, die auf keinen Fall verloren gehen dürfen, ist seit der Einführung 2008 in tausenden Installationen unter anderem in den Bereichen Healthcare, öffentlicher Dienst, Industrie und Handel, sowie Banken und Versicherungen im Einsatz. Der praktische Speicherwürfel ist für zahlreiche Lösungen und nach GDPdU, GoBS und RöV zertifiziert.

Die Silent Brick Library, das flexible „COLD Storage“ mit transportablen Speicher-Containern, setzt ebenso auf die dreifache Absicherung durch Erasure Coding, Digital Audit und Disk Mix. Die Kombination aus linearer Datenstruktur und Festplattentechnologie erlaubt physikalisch trennbare Speicherbereiche und besonders niedrige Speicher-Grenzkosten. Die Silent Brick Library eignet sich besonders für große, aktive Archive, als Backup-Speicher oder als Medienspeicher, z.B. für Videoproduktionen.

FAST LTA ist nach ISO 9001 zertifiziert.

Hallo,

wir sind die **FAST LTA AG**.
Unser Firmensitz ist in der Rüdesheimer Str. 11 in 80686 München, Deutschland. Sie erreichen uns telefonisch unter +49 (89) 890 47 - 0, per Fax unter +49 (89) 890 47 - 890 und via E-Mail über info@fast-lta.de. Beim Amtsgericht München sind wir unter der HRB 127 484 eingetragen, unsere USt-ID ist DE204232266. Die Kontodaten bei der Kreissparkasse München Starnberg sind IBAN DE76 7025 0150 0022 2363 19 und BIC BYLA DE M1 KMS. Im Vorstand sitzen Matthias Zahn, Jörg Adelstein und Reiner Bielmeier, der Vorsitzende des AR ist Dr. Peter van Aubel.
Im Internet finden Sie uns unter **www.fast-lta.de**.