

Hintergrund

Immutable Storage

Cyberangriffe fordern einen stärkeren Schutz von Daten und Backups. Daher liegen unveränderliche Speicher, so genanntes Immutable Storage, im Trend. Dabei ist Immutability – Unveränderbarkeit – gar nicht neu. Wer sich noch erinnert: Schon bei Audiokassetten konnte man durch Ausbrechen einer Lasche auf der Oberseite das Überschreiben verhindern. Neu ist der Einsatz im Bereich

des Objektspeichers, wo Objekte durch so genanntes Object Locking für eine bestimmte Zeit schreibgeschützt werden. Doch auch automatische Snapshots, WORM-Versiegelung und Air Gap sind Methoden, Daten “immutable” zu speichern und so vor ungewolltem oder unberechtigtem Löschen oder Manipulation zu schützen. Worauf kommt es an?



Audio-Kassetten besaßen einen mechanischen „Immutability“-Modus: durch Herausbrechen einer Lasche an der Oberseite war ein Überschreiben nicht mehr möglich.

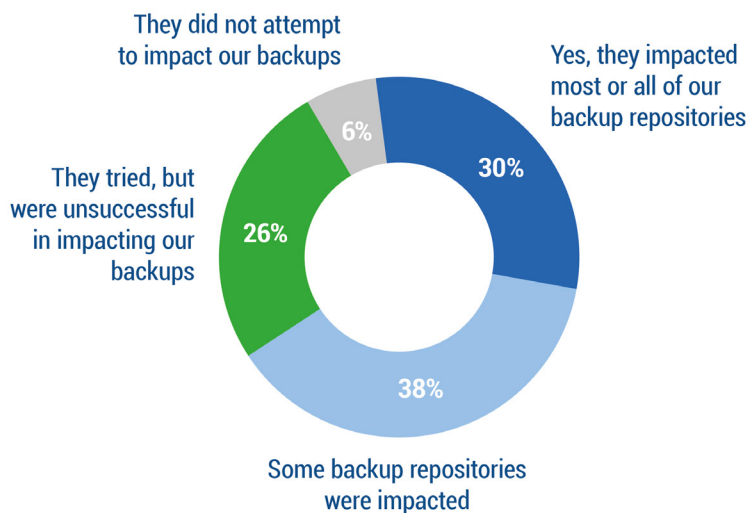
Backups sind besonders gefährdet

Das BSI empfiehlt Backups zum Schutz gegen die Folgen von Cyberangriffen wie z. B. Ransomware. Dennoch genügt es inzwischen nicht mehr, nur auf eine bewährte Backup-Strategie nach dem 3-2-1-Ansatz zu setzen. Nach einer von Veeam veröffentlichten Studie zielen über 90% der Cyber-Angriffe inzwischen auf Backups. Fast 70% der Angriffe sind dabei erfolgreich: es gelingt also, Backups ganz oder teilweise zu verschlüsseln und so unbrauchbar zu machen. Nur knapp ein Viertel der Angriffe konnten vollständig verhindert werden. Veeam kommentiert dies so:

„Deshalb sind Air Gap und Immutability so wichtig.“

Backup Repositories impacted by Attackers

Did the threat actor attempt to modify/delete backup repositories as part of their ransomware attack? (n=1,000)



Source: 2022 Ransomware Trends Report

<https://vee.am/RW22>

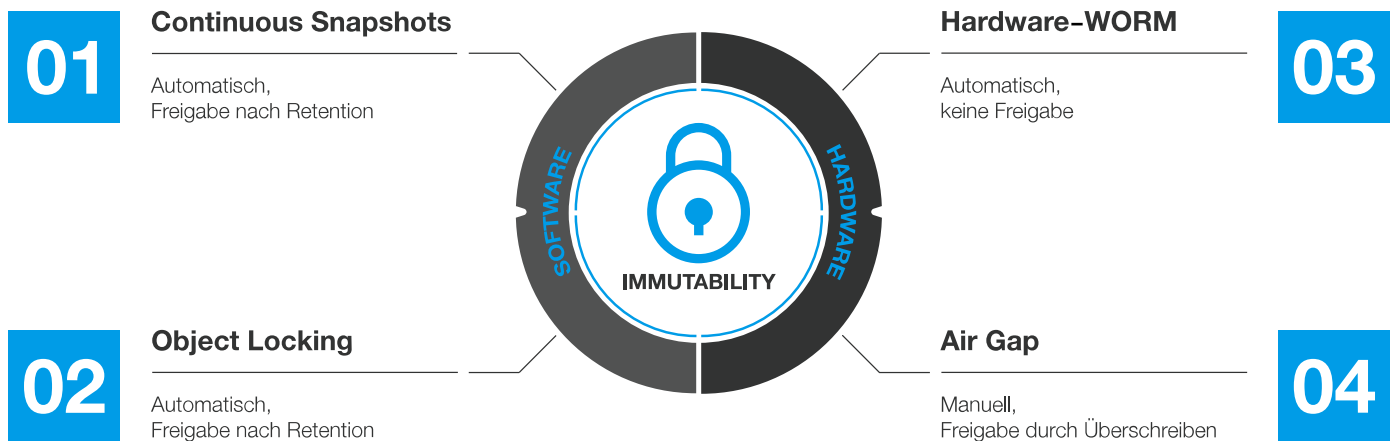
94% der Cyber-Angriffe gingen (auch) gezielt gegen Backups. 68% der Angriffe waren damit (zumindest teilweise) erfolgreich.

Quelle: Veeam

Immutability

Wörtlich bezeichnet Immutability die Unveränderbarkeit von Daten. Einmal geschrieben können diese also weder verändert noch gelöscht werden. Dies muss jedoch nicht, wie z. B. bei echtem Hardware-WORM, durch einen Low-Level-Schreibschutz geschehen, sondern kann mit unterschiedlichen Methoden erreicht werden. Allen Methoden gemeinsam ist: **„Immutable“ Daten sind für Angreifer, ob physisch oder programmatisch, nicht manipulierbar und nicht löschar – oder schlicht nicht erreichbar.**

Folgende Methoden kann man dabei unterscheiden, die jeweils an unterschiedlichen Stellen der Datensicherung sinnvoll eingesetzt werden können, auch in Kombination.



Automatische Snapshots und S3 Object Locking:

Soft(ware)-WORM

WORM – Write Once Read Many, also einmal schreiben, mehrfach lesen – bezeichnet den Schutz eines Objektes, einer Datei, eines Verzeichnisses oder eines Datenträgers gegen Löschen. Dabei gibt es mehrere Möglichkeiten, diesen Schutz umzusetzen. Einfach, aber nicht wirklich sicher ist es, eine Datei via “read only”-Flag zu schützen.

Je nach Rechteverwaltung können Benutzer diesen Schutz leicht wieder aufheben; ebenso können dies Admin-Benutzer. Zum Schutz vor Angriffen ist eine reine Kennzeichnung als „read only“ also eher ungeeignet. Dennoch basieren alle Software-WORM-Schutzmethoden auf einem vergleichbaren Prinzip.

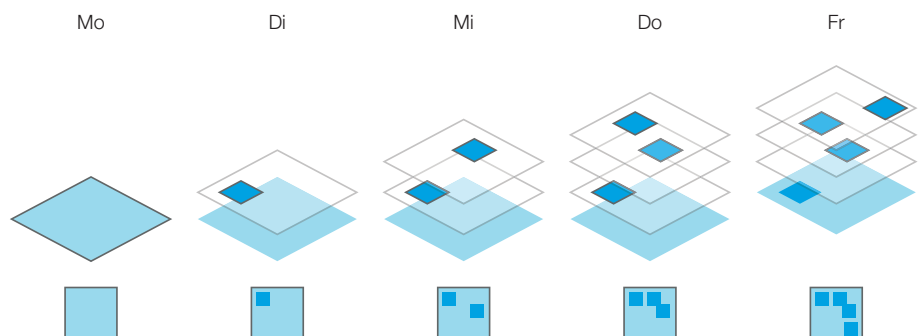
Zum echten Schutz wird diese Funktionalität durch zwei entscheidende Änderungen: Zum einen werden Objekte bei gewünschter “Immutability” (wie z. B. bei automatischen Snapshots oder beim Object Lock) **automatisch von der Logik des Systems abgesichert**, können also auch nicht von den im System vorhandenen Benutzern oder Admins gelöscht werden. Zum anderen wird eine **“Retention Period”**, ein Aufbewahrungszeitraum eingeführt, nach dem der Schutz aufgehoben werden kann oder automatisch erlischt.

01

Continuous Snapshots

Automatisch,
Freigabe nach Retention

Continuous Snapshots funktionieren wie eine Zeitmaschine. Mit jedem Snapshot (hier: täglich) werden die Änderungen zum vorherigen Snapshot gespeichert. Bei Bedarf kann man jeden in einem Snapshot gespeicherten Stand wiederherstellen.



Der grundsätzliche Unterschied zwischen **automatischen Snapshots** mit Retention und **Object Locking** mit Retention ist der Zeitpunkt und die Ansteuerung des Schutzes. Automatische Snapshots werden vom Speichersystem gesteuert und legen bei Veränderungen (auch Löschvorgängen) **neue Abbilder des Speicherzustandes** an, die natürlich zusätzlichen Speicherplatz benötigen. Dadurch ist es möglich, quasi in der Zeit zurückzuspringen und – für eine bestimmte Zeit – jede Veränderung des Datenbestandes granular rückgängig zu machen. Dies ist umso sinnvoller, je „näher“ der so geschützte Speicher an der Datenerzeugung und -Nutzung liegt, da dort Daten noch häufiger (gewollt) verändert oder gelöscht werden. Für weiter entfernte Instanzen der Sicherung, wo sich Daten also nur noch selten oder nie mehr ändern und gar nicht gelöscht werden sollen oder dürfen, werden häufig **Objektspeicher** eingesetzt, die von Haus aus schon wesentlich weniger Speicherplatz benötigen, da nach einem initialen Abbild nur noch Veränderungen (Incrementals) gesichert werden. Objektspeicher haben zusätzlich den Vorteil, dass sie im Vergleich kostengünstiger und im Grunde unbegrenzt skalierbar sind. Das **Object Locking wird von der Backup-Software gesteuert und schützt die geschriebenen Objekte** direkt: Ein Verändern oder Löschen ist innerhalb der Retention schlicht nicht möglich. Nach Ablauf der Retention sorgt die Backup-Software jedoch automatisch dafür, dass die entsprechenden Objekte, nun ohne Object Lock, direkt gelöscht werden. **Damit wird sofort wieder Speicherplatz frei.**

Beide Methoden bieten vor den meisten Angriffen und Manipulationsversuchen hohe Sicherheit.

Dennoch basiert diese "WORM"-Versiegelung rein auf Software – und ist damit potenziell angreifbar. Die Absicherung von Rechten und Accounts liegt dabei in der Hand von Menschen, was Fehler und damit verbundene Sicherheitslücken nicht ausschließt. Empfohlen ist der Einsatz von Zwei- bzw. **Multi-Faktor-Authentifizierung** (2FA bzw. MFA) an jeder relevanten Stelle, um unerlaubten Zugriff zu verhindern.

02

Object Locking

Automatisch,
Freigabe nach Retention

Für S3-Shares lässt sich bei Silent Bricks seit der Software-Version 2.45 optional Unterstützung für Object Locking zuschalten. Buckets können dann (von der verwalteten Software, z.B. Veeam) mit Retention und Immutability versehen werden.

Hardware-WORM

Deutlich weiter geht der Schutz per Hardware. Hier bestimmt die Firmware der Hardware, auf welche Bereiche des Datenträgers schreibend und auf welche nur noch lesend zugegriffen werden kann. Dies wird z. B. im Silent Cube und beim Silent Brick WORM per „Wasserstand“ realisiert: Werden Daten auf einen angeschlossenen Datenträger geschrieben, steigt dieser „Wasserstand“ an. Unterhalb der Markierung führt die Hardware nur noch Lesebefehle aus. **Die Verankerung dieser Funktionalität in der Firmware schließt eine Manipulation aus.**

Allerdings bedeutet dies, dass diese Datenträger stets voller werden, da ja einzelne Daten nie mehr gelöscht werden können – ein Zurücksetzen oder Reduzieren des „Wasserstandes“ ist im Befehlssatz der Hardware schlicht nicht vorhanden. Die Sicherheit ist hierbei jedoch maximal, weshalb Hardware-WORM meistens für Daten eingesetzt wird, die sich nicht mehr oder nur noch selten ändern, wie z. B. bei der Archivierung.

Eine andere Form des Hardware-WORM ist eine physische Sperre, wie z. B. das **Ausbrechen der Lasche bei Audio-Kassetten** oder der Schalter bei SD-Speicherkarten. Da diese physischen Sperren jedoch nur bei Wechselmedien wie Tapes vorkommen, die sowieso manuelles Eingreifen erfordern, und zudem sehr einfach wieder aufgehoben werden können, müssen sie **eher als Schutz vor falscher Anwendung** gelten. Hat ein Angreifer physischen Zugriff auf Wechselmedien, kann der Schreibschutz einfach wieder aufgehoben werden.

Hardware-WORM

Automatisch,
keine Freigabe

03



Silent Bricks gibt es auch mit Hardware-WORM-Versiegelung (links: Silent Brick DS WORM, rechts: Silent Brick WORM). Die mobilen Daten-Container Silent Brick und Silent Brick WORM sind zudem vollständig Air-Gap-fähig.

Air Gap

Apropos Wechselmedien: Eine Art „physisches WORM“ ist der Air Gap, also die **physische Trennung von Medien zum Speichersystem**, wie es z. B. bei Tape oder Silent Bricks möglich ist. Was keine Verbindung mehr zu einem System hat, ist per Definition geschützt – kann aber natürlich dann auch nicht gelesen werden. Für den Lesevorgang muss das entsprechende Medium erst wieder in das System eingelegt werden, was dann auch wieder Schreib- bzw. Löschzugriff erlaubt. Allerdings wird „Air Gap“

mitunter recht freizügig interpretiert. So zählt Veeam auch die Kopie oder **Auslagerung von Daten** in ein separates Rechenzentrum (zweiter Standort) bzw. zu Cloud-Anbietern als Air Gap, unabhängig davon, ob und wie die Daten dort dann für Angreifer erreichbar sind. Um Backup-Daten hier ebenfalls effektiv gegen Manipulation oder Löschen zu schützen, werden Daten auf Objektspeichern mit Object Locking gesichert, womit sich der Kreis wieder schließt.

Air Gap

Manuell,
Freigabe durch Überschreiben

04

Was braucht man?

Offensichtlich lautet die Antwort: **Es kommt darauf an**. Wie so oft gibt es inzwischen nicht mehr die eine Technologie, die jeden Anwendungsfall abdeckt. Sollen Daten langfristig und 100%ig sicher abgelegt werden, z. B. zur rechtskonformen Archivierung, kommt man um Hardware-WORM kaum herum. Aber bei Backup & Recovery ist es meist nicht zielführend, Daten "für immer" aufzubewahren und so den Kapazitätsbedarf unverhältnismäßig zu steigern. Also setzt man hier auf Software-WORM bzw. Immutability.

Je nach verwendetem System und Anbindung kommen von automatischen Snapshots über Air Gap bis zu S3 Object Locking alle Technologien zum Einsatz. Ist physischer Air Gap nicht gewollt oder aufgrund der Datenmengen nicht praktikabel, können Daten auf lokale oder entfernte Objektspeicher ausgelagert werden – diese sollten dann aber unbedingt ebenfalls mittels Object Locking „immutable“ gemacht werden.



Multi-Immutable Storage:

Das Silent Brick System

Das Silent Brick System schützt Daten vor Manipulation und ungewolltem Löschen auf vielfältige Art.

Im File System (SecureNAS) sorgen **Continuous Snapshots** dafür, dass bei Änderungen automatisch neue Versionen angelegt werden. Wie bei einer Zeitmaschine kann man im Ernstfall bis zu 90 Tage alte Versionen wieder herstellen.

Bei der Nutzung als S3-kompatibler Objektspeicher lassen sich Daten per **Object Locking und Retention** schützen.

Silent Bricks bieten bis zu 24 TB Bruttokapazität und sind als **transportables Speichermedium** physisch Air-Gap-fähig, unabhängig von der gewählten Anbindung.

Und auf dem **Silent Brick WORM** mit Hardware-Versiegelung landen all die Daten, die auf keinen Fall verloren gehen oder gelöscht werden dürfen.

Die einzelnen Technologien können je nach Anwendung, Schutzebene und Anforderungen miteinander kombiniert werden. So werden Daten effektiv und über die gesamte Speicherkette gegen Manipulation und unbeabsichtigtes Löschen geschützt.

Das Silent Brick System bietet damit den umfassendsten "Immutability"-Schutz aller Sekundär-Speichersysteme an.

