Unterstützt von

Cronon

iX extra Juni 2022

Storage

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

Backup und Security

Storage im Zeichen von Ransomware

Tape-Libraries: Offline ist nicht immer offline

Seite 121

Backup-Software und -Appliances

Seite 122

Der Cross-over-Punkt von SSD und HDD

Seite 125

Vorschau aufs nächste iX extra: Cloud: Kubernetes-Tools und -Services

Seite 127

iX extra zum Nachschlagen:
www.ix.de/extra

Storage im Zeichen von Ransomware

Ransomware verleiht der Offlinelagerung geschäftskritischer Daten eine neue Relevanz und damit eine neue Dynamik. Die Bedrohung macht Backup und Security zu Verbündeten.

Ransomware-Erpressungen fallen nicht vom Himmel, auch wenn es den Betroffenen so erscheinen mag. Ihnen voraus gehen umfangreiche Erkundungen des geenterten Firmennetzes durch die Angreifer. Meist halten sich diese monatelang in den Zielnetzen auf, um sich von Rechner zu Rechner zu arbeiten und Rechte zu eskalieren. Denn den Einstieg bilden häufig Clientsysteme in einer Fachabteilung, in der sich ein Mitarbeiter eine Schadsoftware einfängt. Die Storage-Systeme stehen am Ende der Erkundungskette und sind das begehrte Ziel. Hier liegen die Daten, durch deren Verschlüsselung die Verantwortlichen erpresst werden.

Grundsätzlich sind zum Schutz gegen Ransomware alle auch sonst empfohlenen Sicherheitsmaßnahmen einzuhalten. Allerdings gelten einige Besonderheiten. Haben die Angreifer bereits einzelne Clientrechner geentert, erschweren ihnen die Trennung unterschiedlicher Netze, etwa von Management- und Datennetzen, eine umfangreiche Zugangssicherung aller Systeme samt striktem Identitäts- und Berechtigungsmanagement und andere Vorbereitungen das Vorankommen im Firmennetz (siehe Abbildung 1).

Wichtig: Je aufwendiger es für die Angreifer ist, sich Richtung Zielsysteme vorzuarbeiten, desto unattraktiver wird eine Firma für die Angreifer und desto höher die Wahrscheinlichkeit, dass diese sich ein leichteres Opfer suchen. Damit ist die Gefahr aber nicht vorbei. Solange sich die Angreifer unentdeckt im Netz bewegen, hält sie nichts davon ab, sich den Zugang offen zu halten und zu einem anderen Zeitpunkt einen neuen Anlauf zu starten.

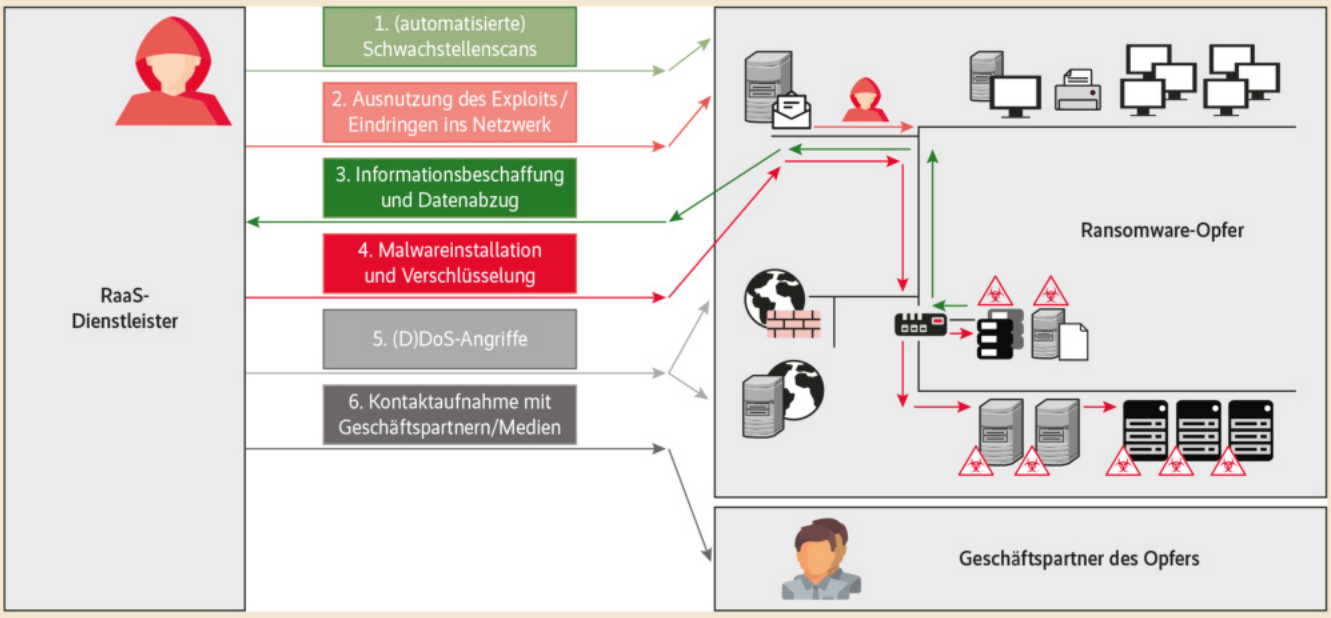
Wenig beachtet ist auch, dass von Ransomware-Erpressern noch andere Gefahren ausgehen. Hat man seine Daten verschlüsselt, schützt das zwar nicht davor, dass Fremde die Daten aus böser Absicht mit einer zusätzlichen Verschlüsselung versehen. Es verhindert aber, dass die Angreifer Daten abzweigen und mit deren Veröffentlichung drohen können. Schließlich sind die Angreifer auf Erpressung aus und nicht wählerisch, was ihre Methoden betrifft.

Neue Verbündete

Vor allem, wenn eine Erpressung mit dem Unbrauchbarmachen der Daten nicht fruchtet, weil intakte Offlinekopien existieren, könnten die Angreifer die vor dem Verschlüsseln heruntergeladene Kopie auf ihr Erpressungspotenzial hin untersuchen und damit einen zweiten Erpressungsanlauf starten. Aus diesem Grund sollten die Verantwortlichen auch ihre on Premises gehaltenen Daten daraufhin untersuchen, welches Erpressungspotenzial in ihnen liegt, sollten sie in die Hände von Erpressern gelangen, und sich gegebenenfalls durch Verschlüsselung davor schützen.

Da es keinen einhundertprozentigen Schutz gegen das unerwünschte Verschlüsseln der eigenen Daten durch Eindringlinge gibt, schützen nur Offlinekopien vor den Erpressungen. Hier werden Datensicherung und Datensicherheit zu Verbündeten. Vor Ransomware hatten beide trotz ähnlich klingender Bezeichnung augenscheinlich kaum mehr miteinander zu tun. Und das gilt leider auch für Security- und Storage-respektive Backup-Experten.

Das kann insofern zu einer Chance für Ransomware-Erpresser werden, als Security-Leute die speziellen Storage-Schnittstellen nicht immer gut verstehen. Was sie verstehen: Eine Datensicherung schützt die Unternehmensdaten vor Veränderung und Verlust, ob vorsätzlich oder unabsichtlich, und muss selbst Ransomware-sicher sein.



Der Weg des Ransomware-Angreifers zu den zu kapernden Daten durchs Firmennetz ist weit und schwierig. Doch je aufwendiger und zeitraubender, desto unattraktiver ist der Erpressungsversuch (Abb. 1).

Quelle: Fast LTA

Die Storage-Container der Silent Bricks sind herausnehmbare Festplattenmagazine, einen Knopfdruck und einen Handgriff von einem Airgap entfernt (Abb. 2).

Die Missverständnisse beginnen beim Begriff „offline", bei der Beurteilung der Medien und der Schnittstellen. Offline heißen klassischerweise Medien, die von ihren Laufwerken getrennt sind. Üblicherweise verstehen Storage-Admins darunter Tapes und optische Medien, wobei letztere vom Aussterben bedroht sind und deshalb im Folgenden außen vor bleiben. Festplatten gelten als Online- oder Nearline-Medien, Halbleiterspeicher als Onlinemedien.

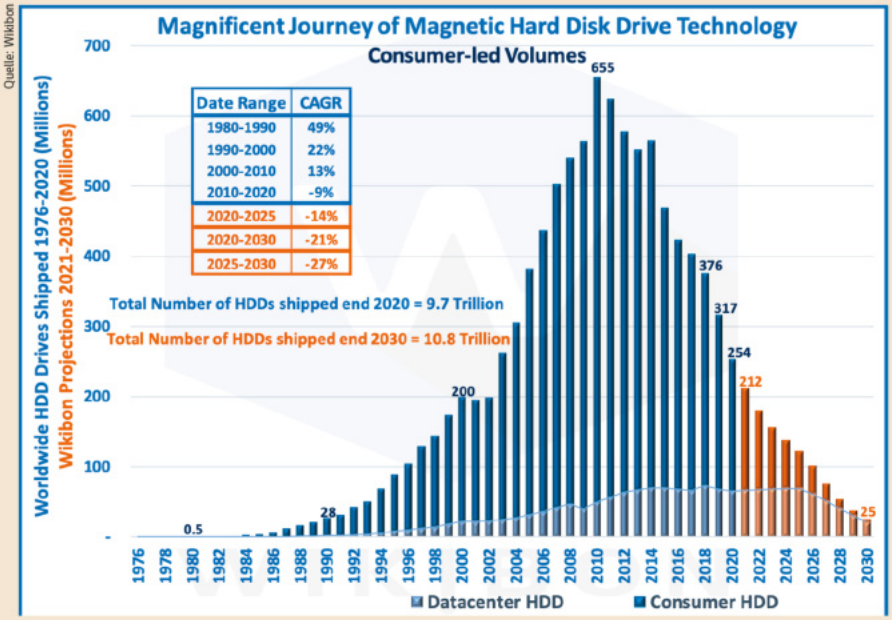
Offline ist nicht immer offline

Offline heißt aber nicht, dass die Medien übers Netz nicht erreichbar sind. Bandbibliotheken und Jukeboxen arbeiten mit Robotern, die mit der geeigneten Software durchs Netz steuerbar sind. Dadurch kann auch ein Unbefugter die Bänder ins Laufwerk einlegen lassen und die Daten überschreiben.

Zudem indiziert die Managementsoftware der Tape-Library die von ihr verwalteten Bänder. Nur so kann sie die von der Backup- oder Archivierungssoftware angeforderten Bänder identifizieren und ins Laufwerk einlegen.

Es gibt zwei Arten der Indizierung: Die Backup-Software indiziert die Inhalte der Bänder, die Library-Software indiziert die Bänder, um sie aus dem richtigen Slot zu holen. Für diese Indizierung existiert eine ganz einfache, gewissermaßen analog-digitale Sicherung: Man versieht die Tapes mit einem Barcode-Aufkleber. Dadurch kann die Bibliothek sie jederzeit mit ihrem integrierten Barcode-Scanner wieder einlesen. Das gilt auch für aus der Library ausgelagerte Bänder, die man per Magazin importiert.

Quelle: Wikibon



Der Markt der Rechenzentrumsfestplatten hat eine andere Dynamik als der für Consumer-HDDs (Abb. 3).

Welche Backup-Daten sich auf dem Band befinden, ist im Barcode nicht hinterlegt. Diese Informationen sind im Index der Backup-Software gespeichert und müssen tatsächlich als gefährdet gelten. Aus diesem Grund sind sie zu sichern, ebenso wie andere kritische Komponenten der IT-Infrastruktur. Schreiben Backup-Anwendungen Metadaten der Sicherung mit aufs Band, müssen sie im Zweifelsfall alle Bänder erst neu einlesen.

Denn eines ist nicht zu unterschätzen: Nutzdaten in Geiselhaft zu nehmen ist nicht die einzige Methode, einem Unternehmen zu schaden. Werden neuralgische Punkte der IT-Infrastruktur beschädigt, kann deren Wiederherstellung derart aufwendig sein und lange dauern, dass dadurch die Produktion empfindlich gestört wird.

Eine Umgebung, die Umgebung hochzuziehen

Ein geeignetes Konzept zu einer umfänglichen Absicherung gegen solche Gefahren

Tape-Libraries

Hersteller	Produkt	URL
Fujitsu	Eternus-Serie	www.fujitsu.com/de/
HPE	StoreEver-MSL-Serie	www.hpe.com
IBM	TS-Serie	www.ibm.com
Overland-Tandberg	NEO Series	www.overlandtandberg.com
Qualstar	Q Series	www.qualstar.com
Quantum	Scalar Series	www.quantum.com
Spectra Logic	T Series	spectralogic.com

Backup-Software und -Appliances

Hersteller	Produkt	Art	URL
Acronis	Acronis Cyber Protect	Software	www.acronis.com
Arcserve	Arcserve Ransomware-Paket	Software/Appliance	www.arcserve.com/de/ransomware-recovery
Barracuda	Barracuda Backup	Software	de.barracuda.com/
Cohesity	Cohesity DataProtect	Software	www.cohesity.com/
Commvault	Commvault Backup & Recovery	Software	www.commvault.com
Dell EMC	Dell EMC PowerProtect Cyber Recovery	Software/Appliance	www.dell.com
IBM	IBM Spectrum Protect Plus	Software	www.ibm.com/products/ibm-spectrum-protect-plus
Micro Focus	Micro Focus Data Protector	Software	www.microfocus.com/
Novastor	Novarstor Enterprise Backup	Software	de.novastor.com
Quest	Quest Backup and Recovery	Software	www.quest.com/
Rubrik	Rubrik Ransomware Investigation	Software	www.rubrik.com
SEP	SEP Sesam Backup	Software	www.sep.de
Unitrends	Recovery Series Backup-Appliances	Appliance	www.unitrends.com
Uranium	Uranium Backup	Software	www.uranium-backup.com
Veeam	Veeam Backup & Replication	Software	www.veeam.com
Veritas	Veritas Backup Exec	Software	www.veritas.com
Zerto (HPE)	Zerto Data Protection	Software	www.zerto.com

besteht darin, eine zweistufige Infrastruktur aufzubauen. Unterhalb der eigentlichen Produktivumgebung liegt der Teil, der notwendig ist, um die Umgebung möglichst schnell wiederherzustellen. Zentraler und wichtigster Bestandteil ist die Backup-Infrastruktur, also alle Systeme, die nötig sind, um die Datensicherungen wiederherzustellen. Dazu gehören auch die Konfigurationen von Systemen, Managed Switches und Routern und andere infrastrukturrelevante Software wie VPN-Gateways, VoIP- oder Zeitserver.

Zu beachten sind auch weitere Ressourcen, die zum schnellen Wiederherstellen der Systeme notwendig sind, etwa DHCP- und TFTP-Server. In automatisierten Umgebungen gehört die Automatisierungssoftware, etwa Ansible, zu den zentralen Komponenten. Vorteil: Sie hält die gesamte Infrastruktur in einem Repository fest und kann sie ohne aufwendiges Eingreifen vonseiten der Admins wieder ausrollen.

Tatsächlich gesichert werden muss dann nur diese Undercloud, der Unterbau, und der von ihr verwaltete Inhalt: Konfigurationen und Images. Die physischen Systeme der Undercloud selbst sollten als Bare-Metal-Images gesichert sein, damit sie auch auf nackter Hardware wiederhergestellt werden können. VMs und Container lassen sich dann schnell ausspielen.

Aber auch für Umgebungen ohne Cloud-Techniken, Container und Automatisierung lohnt es, sie zweistufig mit Unterbau einzurichten und ein Konzept zu entwickeln, wie sich die Produktivumgebung schnellstmöglich wiederherstellen lässt – und die Wiederherstellung zu üben. Beschleunigen lässt sich die Wiederherstellung auch mithilfe eines geeigneten Inventarisierungssystems wie Netbox, einer an die MAC-Adressen gebundenen IP-Adressverwaltung per DHCP und einer Netboot-Infrastruktur. Zusammenpassen muss das Wiederherstellungskonzept – ob es nur gekaperte Daten oder auch Teile der Infrastruktur umfasst – mit dem IRP (Incident Response Plan) des Securityteams.

Eine Lücke aus Luft macht den Unterschied

Im Kontext des Schutzes vor Ransomware-Angriffen meint offline aber eigentlich das Airgap, also eine bewusst geschaffene Lücke zwischen dem Netz und den Datensicherungen. Oft wird behauptet, diese Methode sei zu langsam und deshalb nicht fürs Backup geeignet. Auch dem liegen einige Missverständnisse zugrunde. Ein Airgap sagt nichts über die Medienwahl aus. Häufig sind es tatsächlich Bänder. Sie eignen sich als klassische Offlinemedien gut dazu, außerdem sind Bandbibliotheken auf das Ex- und Importieren von Bändern ausgelegt.

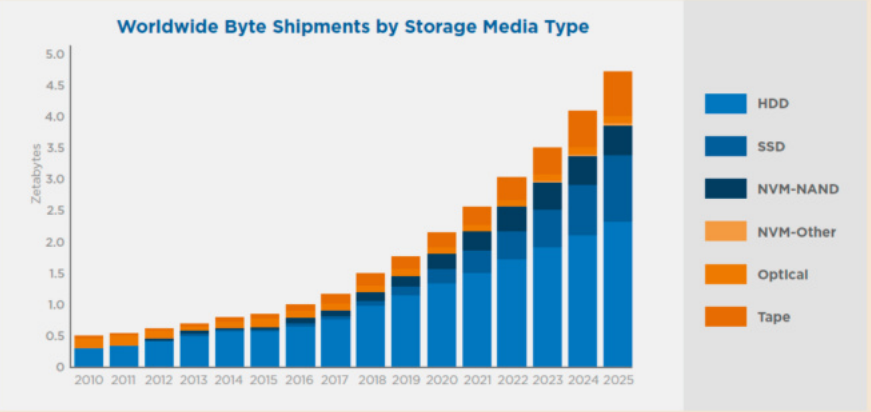
Nutzen lassen sich aber auch Festplatten. Dazu sind spezielle Systeme nötig, die mit dem Herausziehen und Einschieben der Festplatten umgehen können. Am besten eignen sich dazu MAID-Systeme (Massive Array of Independent Disks), die Festplatten herunterfahren. Aktuelle Systeme sind die Silent Bricks von Fast LTA, elastische Speichersysteme mit offlinefähigen, transportierbaren Storage-Containern für Backups und Archive (siehe Abbildung 2).

Die Silent Bricks widerlegen auch die Annahme, das Airgap-Konzept sei zwangsläufig das langsamste. In einem geeigneten Behälter oder Schrank im RZ oder in einem Nebenraum aufbewahrt, ist das Magazin schnell eingeschoben. Das Einbinden der Platten und der Zugriff auf die Daten ist dann eine Sache von Sekunden. Anders bei Tapes in einer Bandbibliothek: Der Roboter hat das Band zwar in wenigen Sekunden ins Laufwerk geschoben, das Spulen zur richtigen Position kann aber Minuten dauern.

Der Nachteil beim Airgap, der ja tatsächlich sein Vorteil ist, besteht darin, dass für jeden Zugriff ein Admin aktiv werden muss, um das Medium in das lesende System einzubinden. Für den häufigsten Wiederherstellungsfall, dass nämlich ein Anwender versehentlich eine Datei oder mehrere gelöscht oder anderweitig verloren hat, ist das tatsächlich zu umständlich. Da aber Mehrfachsicherungen inzwischen Usus sind, lässt sich eine Kopie davon mit Airgap aufbewahren – so auch die dringende Empfehlung.

Alles ist besser als kein Backup

In kleineren Umgebungen kommen häufig USB-Platten als Sicherungsmedien zum



Die Anteile von Flash und Tape steigen unterschiedlich stark, der Anteil der Festplatten fällt (Abb. 4).

Cronon Cloud Services

Hochverfügbar. Sicher. Von hier.

- Storage & Backup für eine robuste Verfügbarkeit Ihrer Daten
- Managed Cloud & Managed Kubernetes für Individualisten
- Beratung & Hosting Service für smarte ERP-Lösungen
- mit EU-Datenschutz und zertifizierter Sicherheit

cronon.net
shift@cronon.net

Cronon

Object-Tape-Storage

Hersteller	Produkt	Beschreibung	URL
Fujifilm	Fujifilm Object Archive	Server-/Clustersoftware, vor eine LTO-Library geschaltet	datastorage-na.fujifilm.com/object-archive/
Quantum	ActiveScale Cold Storage	Objektspeichersoftware mit zweidimensionalem Erasure Coding und Quantum Scalar Tape Libraries	www.quantum.com/en/products/cold-data-storage/
PoINT Software & Systems	PoINT Archival Gateway	Archive-Gateway zwischen S3-Storage und Tape-Library	www.point.de

Einsatz. Sie sind bei IT-Sicherheitsexperten nicht gut angesehen, da diese keine hohe Meinung von der Disziplin ungeschulter Anwender haben. Dagegen sind Storage-verantwortliche Admins sehr wohl in der Lage, regelmäßig ihren Inhalt zu aktualisieren und sie wegzuschließen. Securityspezialisten sollten vor allem nicht vergessen, dass selbst das mit trivialsten Mitteln erstellte Backup besser ist als gar kein Backup.

Vor allem in Industriebetrieben mit kleiner IT-Abteilung muss diese mit den Ressourcen und Schnittstellen zurechtkommen, die sie zur Verfügung hat, und seien es USB, Bluetooth und Mobilfunk. Denn Industriebetriebe sind beliebte Ransomware-Opfer und die in die industrielle Produktion integrierten IT-Systeme mit Zugriff aus dem Firmennetz beliebte Angriffsziele, da sich mit ihnen die Produktion einfach lahmlegen lässt, um so die Firmenverantwortlichen massiv unter Druck zu setzen.

Neben Festplatten und Bändern werden Cloud-Ressourcen für Backups immer beliebter. Man kann zu einem Backup as a Service greifen oder schlicht Speicherplatz in der Cloud mieten, auf den man eine Notfallkopie seiner Backups auslagert. Denn bei Cloud-Storage ist bekanntlich nicht das Lagern, sondern das Herunterladen der Daten oft das Teuerste. Ganz gleich, welche Methode man wählt, entscheidend ist, wie der Zugriff gesichert ist. Die Prämisse muss immer sein, dass sich ein Erpresser unerkannt im eigenen Netz befindet, der Passwörter ausspäht und Zugänge knackt, vor dem also nichts im Netz sicher ist, auch wenn es in Caches oder Logfiles versteckt ist. Geeignete Authentifizierungsverfahren wären etwa MFA (Multi-Faktor-Authentifizierung) mit biometrischen Anteilen. Im Klaren sein sollte man sich aber immer darüber, dass man mit jedem Dienstleister, den man einbezieht, ein weiteres Einfallstor öffnet, nämlich in Form von Supply Chain Attacks.

Eine weitere einfache Möglichkeit, ein Airgap zu schaffen, bietet das LTFS. Mit dem Linear Tape File System lassen sich LTO-Bänder in ein Dateisystem einbinden und damit ähnlich wie eine USB-Festplatte bedienen. Der Vorteil gegenüber Festplatten ist die Modularität: Während das Laufwerk am Rechner verbleibt, lassen sich beliebig viele Medien damit bespielen und anschließend wegschließen. Steigt der Bedarf, kann man das Laufwerk mit einem Roboter in Form eines Autoloader oder einer Bandbibliothek nachrüsten.

Überschreiben unterbunden

Ein weiterer Vorteil von Tape: Alle noch verbliebenen Enterprise-Techniken – das sind nur noch LTO und IBMs Jaguar-Familie – beherrschen ein Firmware-WORM (Write Once, Read Many). Das heißt, man kauft spezielle WORM-Medien, in denen die Weigerung, sich löschen oder überschreiben zu lassen, fest in den Managementchip des Bandes programmiert ist. Die Firmware des Laufwerks liest diese Informationen aus und verbietet ein mehrmaliges Beschreiben des Bandes.

IBM, Mitgründer des LTO-Konsortiums und letzter Hersteller aktueller LTO-Bandlaufwerke, hat etliche Versuche unternommen, Chip und Laufwerks-Firmware zu manipulieren und das WORM zu übersteuern, bisher ohne Erfolg. Selbst wenn das irgendwann gelingen würde, müsste sich der Angreifer physisch in der Opferfirma aufhalten und dort die Geräte aufwendig manipulieren. Da wäre es deutlich einfacher und schneller, die Bänder schlicht zu stehlen.

WORM gibt es auch in Softwareversionen und es gilt bei Archivierungsvorschriften als compliancefähig. Das kann in der Managementsoftware des Storage-Systems oder auf Anwendungsebene implementiert sein. Dennoch ist Software-WORM einfacher und im Zweifelsfall über Netz, also ohne physischen Zugriff, auszuhebeln.

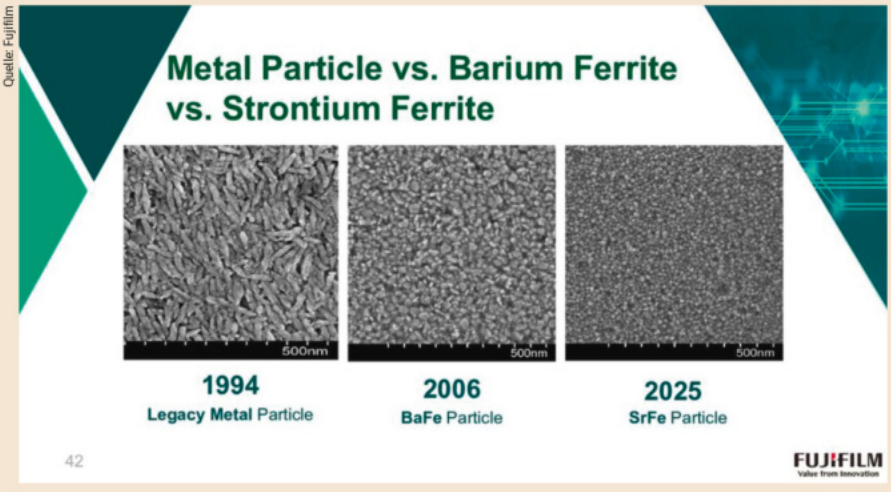
Dasselbe gilt für die neueste Sau, die Storage-Hersteller durch das Ransomware-geplagte Dorf treiben. Immutable Storage funktioniert ähnlich wie Software-WORM: Eine Software entscheidet restriktiv über den Zugriff. Beim Immutable Backup etwa hat nur die Backup-Software Zugriff auf die Bänder, nicht einmal der Admin kann das mit seinen Rechten übersteuern. Doch auch hier gilt dasselbe wie bei Tape-Robotern: Solange eine Low-Level-Schnittstelle existiert, über die sich die vorgesehenen Mechanismen unterlaufen lassen, ist keine einhundertprozentige Sicherheit gegeben.

Lohnt es sich aber für Firmen, die Tapes bereits verbannt hatten oder sich nie mit ihnen anfreunden konnten, noch auf Bänder zu setzen? Ist Tape nicht längst tot? Hier gehen die Meinungen weit auseinander.

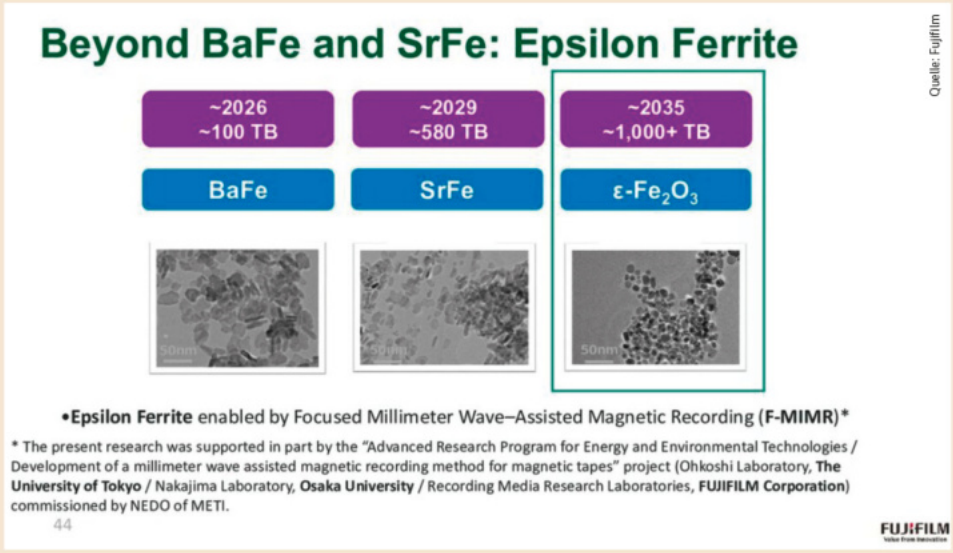
Verkürzte Storage-Hierarchien in Mode

Als klassisch gilt die Storage-Hierarchie, die SSDs als Online-Storage, HDDs als Nearline-Storage und Tape als Offlinespeicher sieht. Vor allem Verkäufer von Festplattensystemen möchten diese Hierarchie gern verkürzen, indem sie behaupten, Festplat-

Quelle: Fujifilm



Mit neuen Materialien lassen sich die Bits auf den Bändern enger aneinanderlegen (Abb. 5).



Mit Epsilon-Ferrite-Bandbeschichtungen will Fujifilm ab 2035 die Bitdichte noch weiter erhöhen und dabei auf Strontium und Barium verzichten (Abb. 6).

ten könnten Tapes ersetzen. Dabei wiederholen sie nur den berühmten Satz des ehemaligen EMC-CEO Mike Ruettgers: „Tape is dead!" – ausgesprochen in den 1990er-Jahren. Seitdem führt das Tape das blühende Leben eines Totgesagten.

Inzwischen ist aber auch die Festplatte längst keine „hippe" Technik mehr. Zwanzig Jahre nachdem die Tape-Technik für tot erklärt wurde, folgte der Abgesang auf den nächsten magnetischen Datenträger. Das Erstaunliche dabei: Nun sollen die HDDs von der einen Seite durch SSDs und von der anderen durch die längst totgesagten Tapes unter Druck geraten – kurz: Nun sollen Flash und Tapes für eine komplette Storage-Hierarchie genügen. FLAPE heißt das Konzept.

Marktanalysten versuchen gern, gewisse Tendenzen und Entwicklungen mit Eckwerten und Zahlen zu belegen. Nach David Floyer, CTO des Analystenhauses Wikibon, werden SSDs bereits 2026 günstiger sein als Festplatten. In seiner Studie „QLC Flash HAMRs HDD" prognostiziert er, dass das Volumen des Festplattenmarkts 2026 nur noch ein Zehntel des heutigen betrage. Bis 2030 sei zudem die Ablösung der Festplatte durch kombinierte FLAPE-Architekturen abgeschlossen.

David Floyer begründet seine Prognose mit dem wirtschaftswissenschaftlichen Wright'schen Gesetz von 1936. Danach erfährt eine Technik bei jeder Verdopplung ihrer Produktionsmenge eine Reduktion der Produktionskosten um einen bestimmten konstanten Prozentsatz. Damit sei der Siegeszug der Flash-Medien und das baldige Ende der Festplatte unausweichlich.

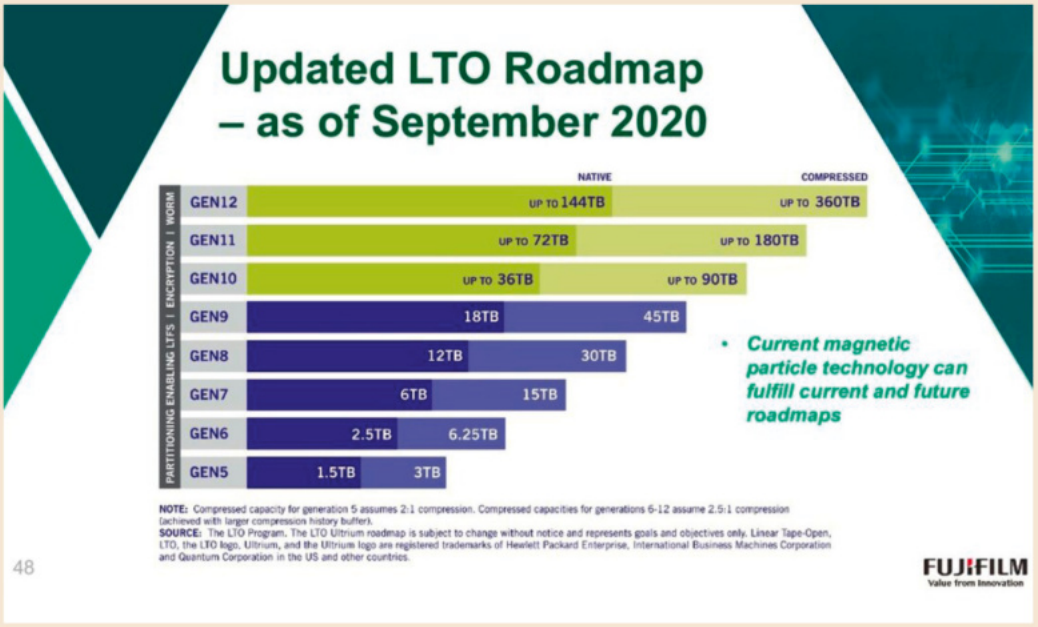
Floyer setzte bereits 2014 auf FLAPE. Vor allem für große Objekte und Dateien kombiniere es niedrigere Kosten mit hoher Performance. Das verändere die Speicherdynamik für langfristige Datenhaltungen und Big Data Lakes.

Der Cross-over-Punkt von SSD und HDD

Dem widerspricht John Chen, Vice President von Trendfocus: Floyer prognostiziere Preissenkungen für Flash, die weit unter den Erwartungen der meisten NAND-Hersteller blieben. Er bescheinigt ihm falsche historische Zahlen, eine irreführende Zusammenstellung der Marktwerte und illusorische Voraussagen zur Markt- und Preisentwicklung. Für ihn werden Festplatten auch in den nächsten Jahren das primäre Nearline-Medium bleiben. Er glaubt, der Markt sei „nicht einmal in der Nähe eines Cross-over".

Unterschiedliche Bewertungen und Prognosen zwischen den Analystenhäusern sind normal, je nachdem, welche Quellen sie zurate ziehen und wie sie die Marktsegmente einteilen. Laut IDC etwa soll der Anteil der Festplatten im Zeitraum von 2018 bis 2024 von 65 auf 54 Prozent fallen, der Anteil der Tapes steigt im selben Zeitraum von 14 auf 18 Prozent und der Halbleiteranteil von 21 auf 28 Prozent (siehe Abbildung 4).

Allerdings lässt sich innerhalb dieser Gesamtbewegung auch ein Gegentrend beobachten. Gartner etwa prognostiziert für die hochkapazitiven Nearline-HDDs bis 2024 kontinuierliche Wachstumsraten im zweistelligen Bereich. Ihre Stückzahl soll bis 2024 jährlich um 39 Prozent wachsen und ihr Umsatz um jährlich 14 Prozent auf 17,1 Milliarden US-Dollar. Insgesamt würde der Anteil der Nearline-HDDs am Festplattenmarkt im Zeitraum von 2020 bis 2024 von 55 auf 84 Prozent steigen.



Bis LTO-12 reicht derzeit die Roadmap des LTO-Konsortiums (Abb. 7).

Währenddessen geht nach Gartner der Marktanteil der hochperformanten Enterprise-Festplatten in den Sinkflug über: Er bewegt sich von 1,8 Milliarden US-Dollar Umsatz im Jahr 2019 bis 2024 auf null. Das Schicksal sollen sie mit Notebook-HDDs teilen. Der Umsatz der Mobile- und Consumer-HDDs soll von 2020 bis 2024 von 3,7 auf 0,8 Milliarden US-Dollar abstürzen. Auch forbes.com sieht den Markt der Nearline-HDDs wachsen, während der Gesamt-HDD-Markt stark schrumpft.

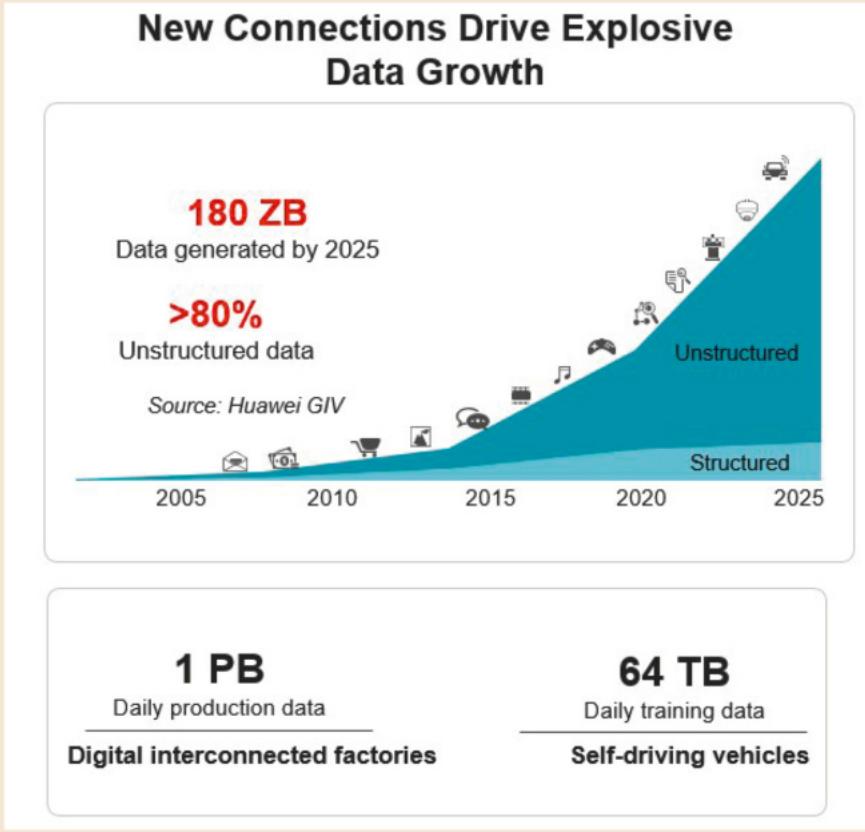
Risiken nicht ausgeschlossen

Deutlich wird dabei, dass die Marktentwicklungen von Consumer- und Data-Center-HDDs nicht kongruieren. Während die Zahl der Consumer-Festplatten seit 2010 so stark schrumpft, dass deren Ende tatsächlich für 2030 zu erwarten ist, wird bei Rechenzentrumsplatten die Trendwende etwa 2025 erwartet und der Schrumpfungsprozess wesentlich langsamer vonstattengehen (siehe Abbildung 3). Gleichzeitig sind die Austauschzyklen der Speichermedien fassenden Systeme im RZ wesentlich länger, dafür ist der Bedarf an – nachzukaufenden – Austauschmedien wesentlich höher. Das alles spricht eher dafür, dass Rechenzentren auch nach 2030 noch Festplatten kaufen werden.

Zu bedenken ist allerdings, dass mit sinkenden Stückzahlen die Produktion für die Hersteller teuer und unattraktiv wird. Dadurch kann die abfallende Kurve des Festplattenmarkts regelrecht einknicken, sobald der SSD-HDD-Cross-over-Punkt erreicht ist, SSDs gleicher Kapazität also günstiger sind als Festplatten. Solche von den RZ-Betreibern nicht beinflussbaren Faktoren erschweren die Prognosen zusehens. Allen voran die Verfügbarkeit und die damit verbundene Kostenentwicklung von Halbleitern ebenso wie die Beschaffungsrisiken benötigter Rohstoffe und andere Verknappungen können den SSD- und HDD-Markt in den nächsten Jahren wild durcheinanderwürfeln.

Geringer sind die Beschaffungsrisiken bei Bändern. Aktuelle Generationen besitzen magnetische Beschichtungen aus Bariumferrit, sie enthalten Eisen, Chrom und Barium – keines davon fällt unter die kritischen Rohstoffe. Zudem fällt der Bedarf an Metalloxiden pro Kassette bei einer Schichtdicke von 10 nm mit 0,7 Gramm eher gering aus. Dafür erreicht die aktuelle Generation LTO-9 18 TByte unkomprimiert. Anders als bei Festplatten ist hier noch viel Luft nach oben.

Fujifilm beispielsweise plant ab 2029 den Umstieg auf eine Strontiumferrit-Beschichtung (siehe Abbildung 5). Das könnte die Kapazität auf bis zu 580 TByte erhöhen: Der mit IBM Research zusammen aufgestellte Rekord für Magnetbänder liegt bei einer Flächendichte von 317 GBit pro Quadratzoll. Eine Verdoppelung der Flächendichte soll danach mit Hexaferrum respek-



Quelle: Huawei

Vor allem die Menge der unstrukturierten Daten wächst ungebremst. Ob die alle – mehrfach – gesichert werden müssen, sollte gut überlegt sein (Abb. 8).

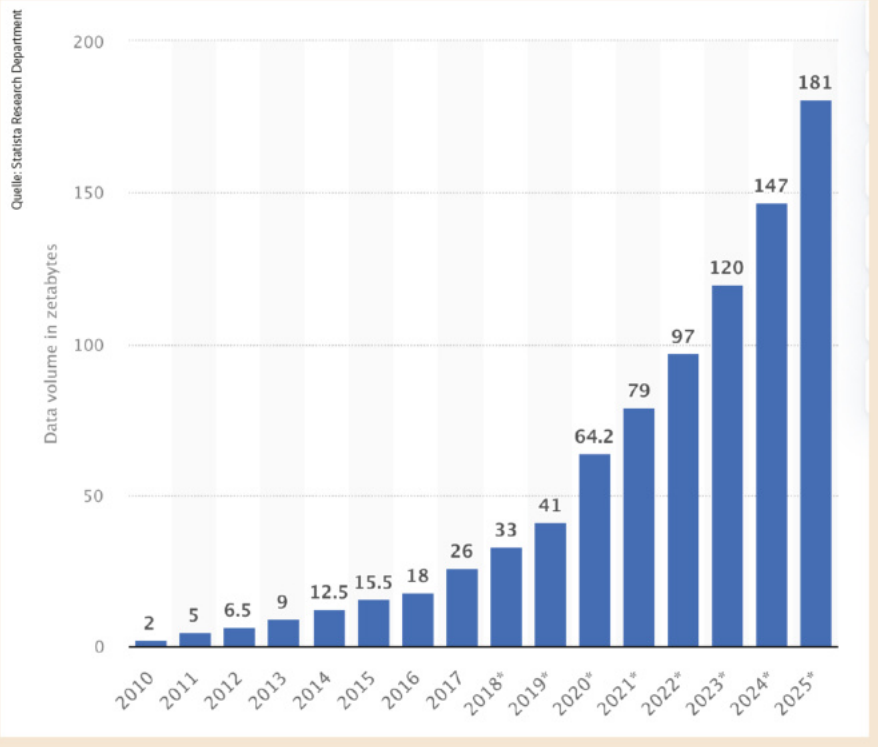
tive Epsilon Ferrite als magnetischer Beschichtung mit noch feineren Partikeln in Verbindung mit der Aufnahmetechnik F-MIMR (Focused Millimeter Wave-Assisted Magnetic Recording) gelingen (siehe Abbildung 6). Erwartet wird die Technik ab 2035.

Auch das LTO-Konsortium lässt keinen Zweifel an der Zukunftsträchtigkeit von LTO: Dessen Roadmap reicht bis LTO-12 (siehe Abbildung 7). Zudem geht Tape mit allen anderen Speichertechniken Verbindungen ein: mit Blockgeräten wie Festplatten über LTFS, mit Flash als FLAPE und mit der Cloud in Form von Object-Tape-Archiven. Wie lohnend Investitionen in die Entwicklung neuer Bandaufzeichnungsverfahren sind, zeigen wieder die Marktprognosen.

Das Tape Storage Council meldete für 2019 einen neuen Rekord mit über 225 Millionen verkaufter Bänder und 4,4 Millionen Laufwerken. Dies entspräche einem jährlichen Wachstum von 33 Prozent, weit über dem Durchschnitt aller Medien. In den letzten zehn Jahren habe LTO zudem seine Kapazität um 1400 Prozent gesteigert. In einer Studie der Enterprise Strategy Group gaben 61 Prozent der Unternehmen 2020 an, ihre Investition in Tape in der bisherigen Höhe fortführen oder ausbauen zu wollen.

Backup und Ransomware-Schutz sollte sich also nicht an bestimmten Medientypen orientieren. Das spiegelt auch die 3-2-1-1-Backup-Regel wider: drei Backup-Kopien auf zwei unterschiedliche Medientypen und idealerweise noch je eine Offsite- und eine Offlinekopie. Aber: Bei den Datenmassen ist das nicht immer praktikabel. Vor allem die Menge der unstrukturierten Daten wird noch weiter stark wachsen (siehe Abbildung 8). Zuletzt schätzte die IDC den Anstieg der weltweiten Datenmenge bis 2025 auf 180 ZByte (Zettabyte) – ausgehend von 64 ZByte im Jahr 2020. Etwas genauere Zahlen lieferte das Statista Research Department im März 2022: 2021 waren es 79 ZByte, 2022 sollen es 97 ZByte sein, 2023 dann 120, 2024 schon 147 und 2025 ganze 181 ZByte (siehe Abbildung 9).

Diese großen Mengen unstrukturierter Daten haben zudem ihren Anteil daran, dass Backup und Archivierung in der Praxis weiter verschwimmen. Dazu tragen auch Object-Tape-Archive bei, die Cloud-Object-Storage auf Tapes auslagern (siehe Tabelle „Object-Tape-Storage“). Umso wichtiger ist es, zu unterscheiden, ob es sich um businesskritische Daten handelt, also Geschäfts-, Produktiv- und personenbezogene Daten, oder um Daten, die man lediglich für eine eventuelle spätere Analyse aufbewahren will. Hier die 3-2-1-1-Backup-Regel anzuwenden, wäre tatsächlich mit Kanonen auf Spatzen geschossen.



Die jüngste Prognose veröffentlichte das Statista Research Department am März 2022. Danach existieren 2025 bereits 181 ZByte Daten (Abb. 9).

Über Speichermedium und -system, Lagerort und Zugriffsaufwand kann nur der Wert der Daten entscheiden und nicht die Anti- oder Sympathie für oder gegen eine bestimmte Technik. Deshalb besteht die wichtigste und erste Aufgabe eines jeden Verantwortlichen darin, den Wert und die Relevanz der Daten zu analysieren und festzulegen, wie wichtig sie für das Fortbestehen der Firma, für eine unterbrechungsfreie Produktion und für das Einhalten von Vorschriften sind, ob diese nun den Datenschutz, die Steuer oder die Dokumentationspflicht betreffen. *Susanne Nolte* (sun@ix.de)