

storage-magazin.de

Eine Publikation von ***speicherguide.de***

Storage für den Mittelstand

2024

03

Datenspeicherung neu ausrichten

Editorial

STORAGE KANN IMMER MEHR – DIE ANFORDERUNGEN BLEIBEN ABER KOMPLEX



Karl Fröhlich
Chefredakteur
speicherguide.de

Mit unserer »Storage-Brille« sind wir natürlich parteiisch, wenn wir behaupten, dass es nicht egal ist, auf welchem Speicher Daten gespeichert werden. Darüber, ob nun Storage, Server und/oder Netzwerke der wichtigere Baustein in der IT-Infrastruktur sind, lässt sich trefflich diskutieren und hängt letztendlich vom jeweiligen Einsatzspektrum ab. Ohne Daten sind alle drei nutzlos. Es kommt also auf das Miteinander an.

Ich denke wir sind uns einig, dass das Datenwachstum unaufhaltsam ist. IDC zufolge wurden 2022 rund 3,4 PByte/s an Daten generiert. In drei Jahren sollen es 9,2 PByte/s sein. Wobei die Analysten im Detail nicht nur von neu erzeugten Daten sprechen, sondern hier auch alle Daten dazu packen, die geändert bzw. konsumiert wurden.

Andere Vorhersagen sprechen davon, dass im kommenden Jahr bis zu 175 ZByte und mehr erzeugt werden. Wie genau diese Prognosen eintreffen, ist eigentlich nebensächlich. Ob weltweit zehn, 50 oder 100 ZByte mehr oder weniger generiert werden, ist für uns als mittelständische Unternehmen nebensächlich. Für uns gilt es, mit den vorhandenen Mitteln das Maximale herauszuholen.

Im Marketing-Sprech bedeutet dies, »eine moderne IT-Umgebung muss den steigenden Anforderungen an Effizienz, Flexibilität und Skalierbarkeit gerecht werden.« Klingt erstmal sinnvoll, ist es auch, in der Praxis aber oft gar nicht so einfach umzusetzen. Andererseits sind heute alle Speicher skalierbar und mit hybriden Systemen auch

relativ flexibel. Namhafte B-Brands bieten zusammen mit ihren Vertriebspartnern All-Flash-Lösungen und bezahlbare NVMe-iSCSI-SANs an. Die einzelnen Serien sind mittlerweile ebenfalls gut miteinander kombinierbar. Die nächsten Produktgenerationen werden den Unified-Gedanken noch weiter entwickeln und neben File und Block auch Object in ein und demselben System abhandeln.

Die Produkte können immer mehr und nehmen uns ein Stück Arbeit ab. Einfacher wird das Management künftig trotzdem nicht. Je mehr im Unternehmen mit den gespeicherten Daten gearbeitet werden soll, desto komplexer. Gleichzeitig erhöht die Gesetzgebung die Anforderungen in puncto Cybersicherheit (NIS-2) und der Markt selbst ist auch immer für Kapriolen gut. Nachdem Broadcom das Vmware-Geschäft bewusst gegen den Mittelstand positioniert, wartet hier sehr viel (ungeplante) Arbeit auf nahezu alle IT-Abteilungen.

Wir fassen die Lage im Storage-Markt für Sie zusammen. Beim Lesen dieser Ausgabe wünsche ich Ihnen viel Spaß, neue Erkenntnisse und Inspirationen. Wie immer gilt, teilen, liken und verbreiten ist mehr als erwünscht. Für Anmerkungen, Ideen und Vorschläge stehen wir gerne zur Verfügung.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Bild: ChatGPT/DALL-E



SEITE
5

Datenspeicherung & Storage-Management neu ausrichten

STORAGE ZENTRALER BAUSTEIN DER IT-INFRASTRUKTUR

Storage-Systeme sind zentral für die Leistung und Anpassungsfähigkeit moderner IT-Infrastrukturen und mehr als nur Datenspeicher. Mit wachsenden Datenmengen und steigenden Anforderungen an Flexibilität und Effizienz sehen sich Unternehmen gezwungen, ihre Speicherstrategien zu überdenken bzw. ihr Storage-Management neu auszurichten.

NIS-2-Richtlinie nimmt Geschäftsleitung in die Pflicht

GESETZLICH VERORDNETE CYBERSICHERHEIT



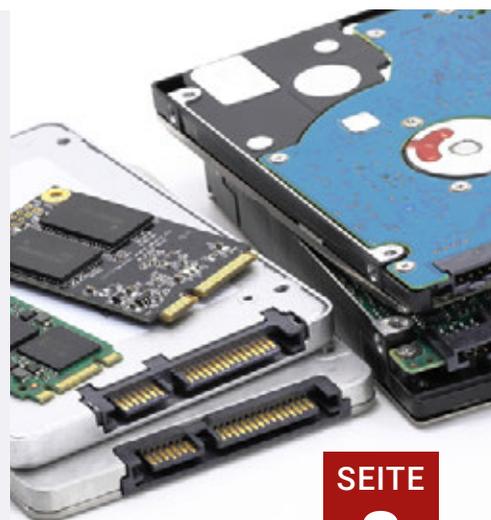
Bild: via Canva Pro

SEITE
21

»Es gibt einfach keinen Grund mehr, HDDs zu kaufen« – oder doch?

FLASH VS. HDD: ARGUMENTE FÜR BEIDE TECHNOLOGIEN

Speicherkapazität, Geschwindigkeit und Kosten pro GByte waren bisher die Disziplinen in dem Dreikampf, den sich Flash-Storage und HDD-Storage lieferten. Die Flash-Fraktion räumt der Festplatte künftig keine Chancen mehr ein. Das HDD-Lager sieht dies selbstredend anders. Vielmehr könne Flash dem Datenwachstum nicht annähernd gerecht werden.



SEITE
8

Bild: ChatGPT/DALL-E

Übersicht Storage-Anbieter



SEITE
11

Editorial	3
Datenspeicherung	
Storage zentraler Baustein der IT-Infrastruktur	5
Flash vs. HDD: Argumente für beide Technologien	8
Übersicht Storage-Anbieter	11
Advertorial	
actidata T-Pontis – Jetzt wird »gebridged«	12
Ohne Daten kein Geschäft	13
Ab auf die Überholspur: 10 Gründe für NVMe-SANs im Mittelstand	15
Silent Bricks mit Fast Clone Support für Veeam	17
actidata DX6-Produktfamilie – Einfach mal Backup machen	19
Cybersicherheit	
Gesetzlich verordnete Cybersicherheit	21
Datenspeicherung	
Storage für KI im Mittelstand	25
Infrastruktur	
Vmware aktuell (noch) unumgänglich	29
Service	
Impressum	32

Sicheres Backup als Schutz vor den Folgen von Ransomware Attacken

Ein Angriff durch Ransomware ist für ein Unternehmen immer eine Katastrophe. Allein das Schützen des Netzwerk vor weiteren Angriffen erfordert oft viele Tage. Ist dann auch noch das Backup der Unternehmensdaten von der Attacke betroffen, kann das den Ruin bedeuten.

Den besten Schutz des Backups bieten natürlich nach wie vor **ausgelagerte LTO-Kassetten**, da hier jede Art von Remote-Zugriff zu 100% ausgeschlossen werden kann. Auch bei Libraries sollten die Kanister mit dem Backup am besten entnommen werden.

Doch auch die Hersteller von **diskbasiertem Backup** haben einiges getan, den Zugriff auf die Datensicherungen zu verhindern. Minimum der Anforderungen ist, dass die Daten nur für die Backupsoftware selbst sichtbar sind. Das ist z.B. bei **Open-E JovianDSS** der Fall, wenn die Daten snapshotbasiert auf einen weiteren Rechner gesichert werden.



EonStor GS 1000 Gen2

Ebenso macht es mittlerweile auch **Infotrend** mit ihren **EonStor GS** Systemen. Hier kommt eine **Data-Lock** Funktion dazu, die Backup-Volumes unveränderlich macht.

Außerdem bietet Infotrend die

Möglichkeit, selbständig Backups zu ziehen, sowie **S3 Immutable Backupvolumes für Veeam** zur Verfügung zu stellen.

Sehr elegant hat das **ExaGrid** gelöst: Hier werden die Backups nach Auslagerung in eine **zweite Repository-Ebene** (mit Deduplikation

auch über viele Knoten) gesichert. Dort können sie mit einer einstellbaren **Retention Time** vor jeder Veränderung geschützt werden. Bei **Veeam**, der idealen Software für die Sicherung virtueller Maschinen, lässt sich ein Linux Server zum **Hardened Linux Immutable Repository** machen, das nur von der Software direkt erreicht werden kann und ebenso durch Retention Zeiten geschützt wird.

Backuplösungen mit Schutz vor Ransomware bei EUROstor:

(mehr Info unter www.EUROstor.com/backup.)

- **LTO Tape Libraries von Actidata**
Schutz der Daten durch räumliche Auslagerung 
- **Veeam Backup Server**
Zweit-Sicherung der Virtuellen Maschinen in ein Immutable Repository (s. rechts) 
- **ExaGrid Tiered Backup Storage**
Backups mit Retention in einer zweiten Backupenebene 
- **Infotrend EonStor GS**
Volumecopy mit Schreibschutz durch Data-Lock Funktion und als S3 Speicher für Veeam Repository 
- **Open-E JovianDSS Storage**
snapshot basierte On-/Off-site Data Protection (ODP) auf zweiten Standort 



Alle Storage-Systeme aus einer Hand:

EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, Scale-Out Clustern und Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die

Virtualisierung. Dazu kommen RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches.

Rufen Sie uns einfach an, wir beraten Sie gerne! Registrieren Sie sich auch für unseren Storage Newsletter (Print oder E-Mail, 3 x pro Jahr) unter www.EUROstor.com/Newsletter.



VEEAM AMD EPYC



ES-3036 als Hardened Linux Immutable Repository mit 36 Slots (12 davon auf der Rückseite)

ES-3036, 36 3.5" Slots, z.B. teilbestückt mit **€ 13.078,10** (inkl. MwSt.) **€ 10.990,-** (exkl. MwSt.)
12 x 20 TB SATA Enterprise HDDs,
2 x 512 GB M.2 Boot-SSD für das Betriebssystem

Hardened Linux Backup Repository Server:

- Storage-Server mit 36 3.5" Slots, bis 864 TB bei Verwendung von 24 TB Disks
- alternativ: 12/16/24 3.5" Slots, 24/72 2.5" Slots
- AMD EPYC Rome 7232P Prozessor, 8 Core, 3,1 GHz auf Supermicro H12SSL-NT Board, 7 PCIe 4.0 Slots
- 64 GB RAM, optional bis zu 1 TB
- 2 x 10 GbE (RJ45) onboard, opt. mehr und bis 100 GbE
- OS auf 512 GB NVMe M.2 SSDs im RAID 1, Ubuntu auf Wunsch vorinstalliert
- Areca RAID Controller mit 12 Gbit SAS, RAID Management über dedizierten Netzwerkport
- optional Erweiterungports für bis zu 512 Laufwerke
- Monitoring, remote Management und iKVM Console über Netzwerk (IPMI)
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt • Tel: +49 (0)711 70 70 91 70 • Fax: +49 (0)711 70 70 91 60

Preisänderung, Druckfehler und Irrtum vorbehalten.

Informieren und registrieren Sie sich auf unserer Website: www.EUROstor.com/Newsletter

E-Mail: Info@EUROstor.com - Tel.: +49 (0)711 70 70 91 70

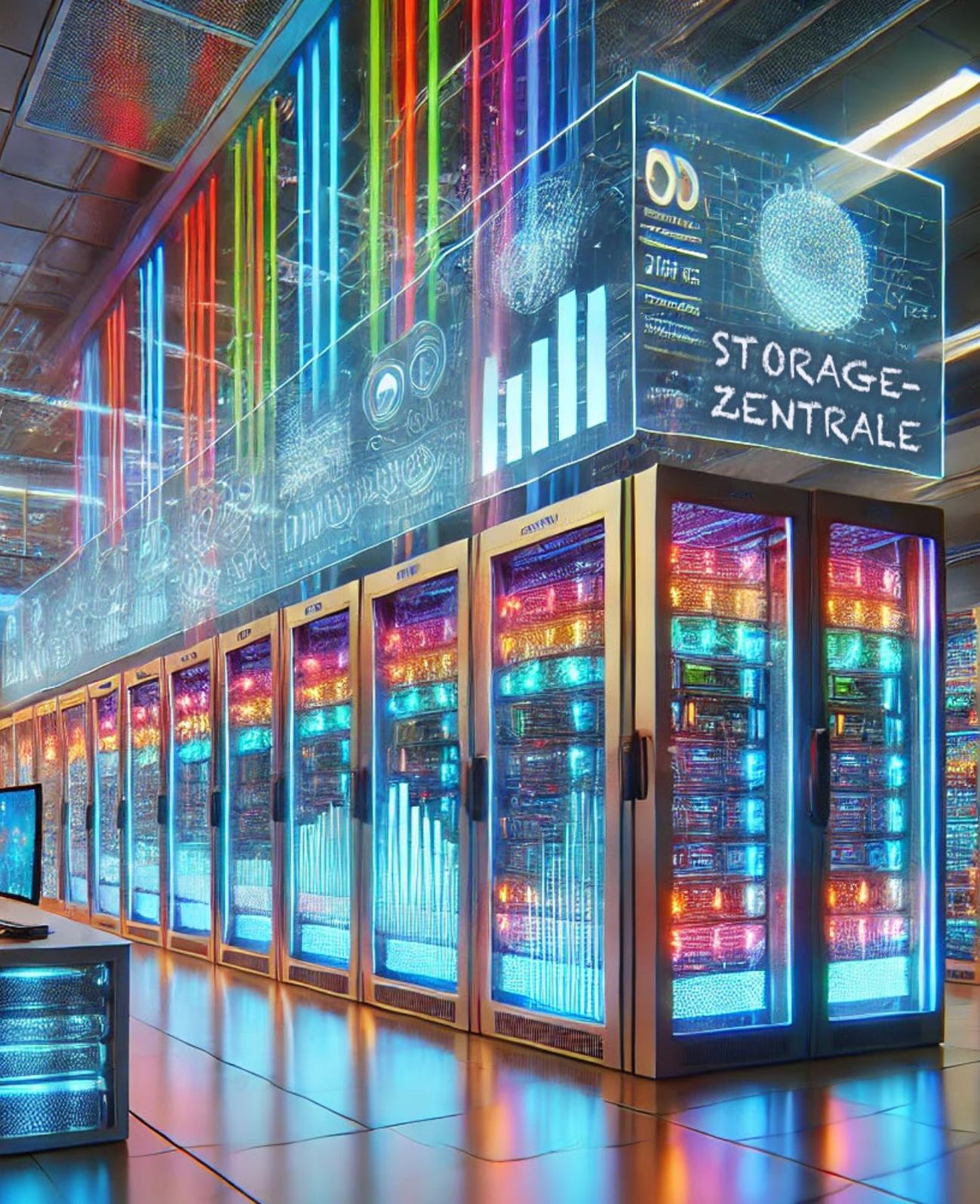


Bild: ChatGPT/DALL-E



Karl Fröhlich
speicherguide.de

Datenspeicherung & Storage-Management neu ausrichten

STORAGE ZENTRALER BAUSTEIN DER IT-INFRASTRUKTUR

Storage-Systeme sind zentral für die Leistung und Anpassungsfähigkeit moderner IT-Infrastrukturen und mehr als nur Datenspeicher. Mit wachsenden Datenmengen und steigenden Anforderungen an Flexibilität und Effizienz sehen sich Unternehmen gezwungen, ihre Speicherstrategien zu überdenken bzw. ihr Storage-Management neu auszurichten.

Storage nimmt seit jeher einen zentralen Stellenwert in der IT-Infrastruktur ein. Nicht zuletzt, weil Daten und Programme gespeichert sein wollen. Mit stetig wachsenden Datenmengen und der zunehmenden Digitalisierung aller Geschäftsbereiche nimmt die Bedeutung von leistungsfähigen und skalierbaren Speicherlösungen seit Jahren weiter zu.

Wobei es zum Thema Storage durchaus konträre Stimmen gibt: Die Einen bezeichnen Storage als Commodity und künftig würde sowieso alles in einem großen Pool gespeichert. Wobei hier eher das eigene Vertriebsmodell der Vater der Gedanken sind. Dazu gehört vor allem die Cloud-Fraktion, aber auch All-Flash-Anbieter versteigen sich in der These, dass sich Preise und Unterschiede soweit angleichen, dass künftig alle Speicherbedürfnisse mit Flash abzudecken seien. Seriöse Storage-Experten haben jedoch Schwierigkeiten damit, dieser Argumentation zu folgen.

Storage als Grundlage für Geschäftsmodelle

»Storage ist nicht mehr nur ein Mittel zur Datenablage, sondern ein entscheidender Faktor für die Leistungsfähigkeit und Flexibilität moderner IT-Umgebungen«, erklärt **Stefan Roth**, Data Storage Business Manager Germany bei **Fujitsu**. »Da unterschiedlichste Applikationen und Anwendun-



Foto: IBM

Rald Colbus
IBM

»Viele Firmen migrieren die Daten wieder aus der Cloud ins Datacenter. Die Treiber hierfür sind Kosten, Security, Compliance, Performance.«

gen auf eine zuverlässige und effiziente Speicherinfrastruktur angewiesen sind, wird Storage immer wichtiger. Dies gilt besonders für den Mittelstand, der mit begrenzten Ressourcen oftmals mehr erreichen muss. Effiziente Speicherlösungen ermöglichen es mittelständischen Unternehmen, ihre IT-Budgets optimal zu nutzen, die Betriebskosten zu senken und dennoch eine hohe Verfüg-



Foto: speicherguide.de

Marc Kleff
Netapp

»Storage ist und bleibt essentiell, weil das Thema über einfache Datenspeicherung weit hinausgeht.«

barkeit und Performance sicherzustellen. In diesem Kontext bietet Storage nicht nur die Grundlage für speichern, managen, sichern und wiederherstellen, sondern auch für innovative Geschäftsmodelle und die schnelle Anpassung an sich verändernde Marktanforderungen.«

»Die Bedeutung von Daten ist für nahezu jedes Unternehmen und jede Organisation in den letzten Jahren



Foto: speicherguide.de

Stefan Roth
Fujitsu

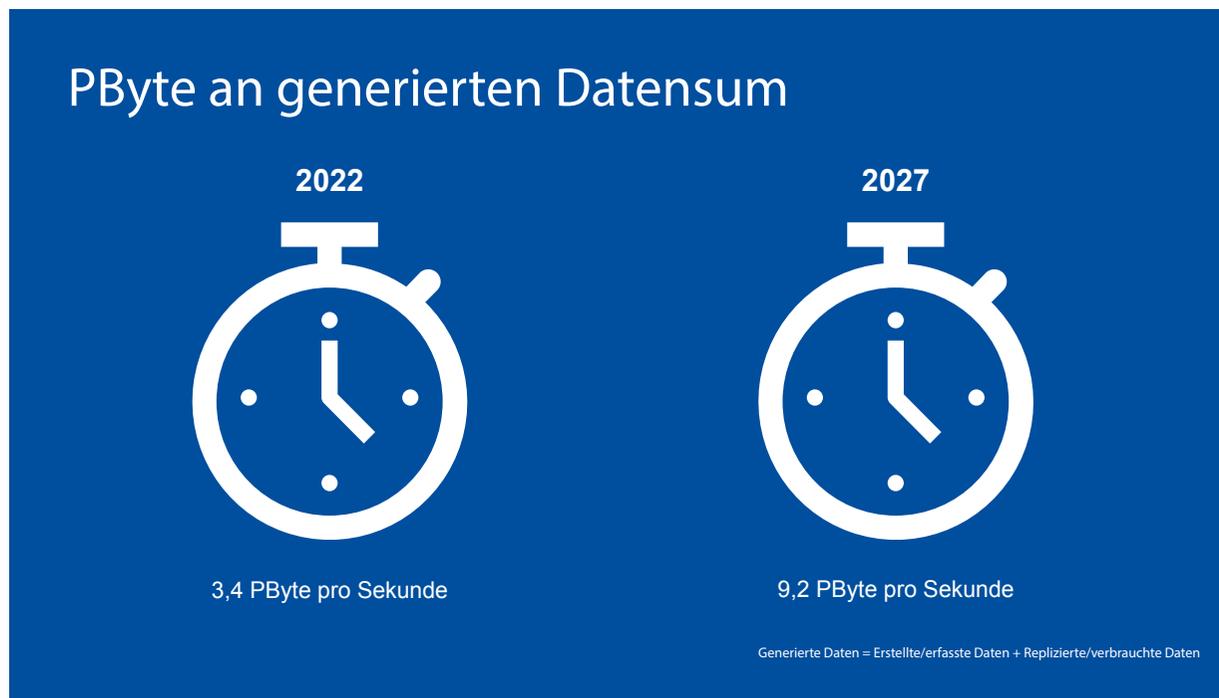
»Automatisierung und KI zur Optimierung von Speicher-Ressourcen und zur Vorhersage von Speicheranforderungen gewinnt an Bedeutung.«

deutlich gewachsen«, ergänzt **Marc Kleff**, Director Solutions Engineering bei **NetApp**. »Die schiere Menge ist natürlich ein Thema. Aber auch die Auswertbarkeit, sprich die Informationsgewinnung, ist eine echte Herausforderung; nicht zuletzt, weil sich der Datenraum bis heute deutlich und ständig erweitert. Daten fallen immer und überall an, sowohl im geschäftlichen als auch im Consumer-Umfeld.

Entsprechend spannt sich der Datenraum heute von IoT-Devices und dem Edge über die Rechenzentren in die Cloud – das ist ein hochdynamisches Umfeld. Wenn ich nun als Organisation jeglicher Art aus diesen Daten das Beste herausholen möchte, seien es beispielsweise betriebliche Kennzahlen, KI-Erkenntnisse und Applikationsbetrieb, brauche ich eine intelligente Dateninfrastruktur. Kurz, Storage ist und bleibt essentiell, weil das Thema über einfache Datenspeicherung weit hinausgeht.«

Ralf Colbus, Principal Storage Technical Specialist bei **IBM Storage Team DACH**, sieht es ähnlich: »Wenn Storage Commodity wäre, würde faktisch ja auch jeder Workload bzw. jede Applikation gleichbehandelt werden und auch dieselben Ansprüche an die Storage-Architektur und Technik haben. Ein Beispiel: Eine Anforderung für KI (AI) an ein Speichersystem kann bei 320 GByte/s zu erreichendem Durchsatz liegen, das ist eine andere Klasse als ein Netzwerkspeicher, auf dem ab und zu eine Powerpoint abgelegt wird. Für Edge-Computing benötigen wir ebenfalls andere Storage-Klassen als im Datacenter. Wir benötigen also dedizierte Systeme, die unter anderem gemäß Latenz, Durchsatz und Verfügbarkeit optimiert sind. Das ist keine 'Commodity'.«

Vielmehr werde Storage immer wichtiger, vor allem in Bezug auf



künstliche Intelligenz und Sicherheit sowie in Hybriden-Umgebungen. Die »one-size-fits-all«-Lösung wird es laut Colbus nicht geben: »Für viele Kunden ist auch das Cloud-Paradigma nicht aufgegangen – sie migrieren die Daten wieder aus der Cloud ins Datacenter. Die Treiber hierfür sind Kosten, Security, Compliance, Performance.«

Datenverwaltung immer komplexer

Tendenziell bleibt Storage also im Fokus der IT-Abteilungen. Dies liegt vor allem an dem zu erwartenden

Datenwachstum. Den Marktforschern von **Statista** zufolge könnten bis 2025 mehr als 175 ZByte an Daten erzeugt werden. Aktuell würde dies unsere Fähigkeit, diese zu speichern an seine Grenzen bringen.

Und es wird noch schlimmer: **IDC** zufolge werden 2027 bis zu 9,2 PByte/s generiert. Vor zwei Jahren waren es noch 3,4 PByte/s. Hierbei handelt es sich nicht ausschließlich um neu erstellte Informationen, die Marktforscher zählen auch Daten hinzu, die geändert bzw. »angefasst« wurden.

Zudem fällt das Datenwachstum nicht mehr vor allem im Consumer-Bereich an: »Bis 2027 sollen 80 Prozent aller Daten in Unternehmen generiert werden«, sagt Netapp-Manager Kleff.

Gleichzeitig nimmt auch die Komplexität der Datenverwaltung zu. Laut Fujitsu-Manager Roth wachsen zudem die Anforderungen an Datensicherheit, Verfügbarkeit und Performance: »Aber auch Regularien wie NIS-2 und DORA sowie die Integration von Cloud-Speicherlösungen, die Ver-

waltung hybrider Speicherumgebungen und die Implementierung von Technologien wie Künstliche Intelligenz und maschinelles Lernen zur Optimierung der Speicherverwaltung erfordern spezialisierte Kenntnisse und kontinuierliche Weiterbildung.«

Vor einigen Jahren gab es vermehrt Silos, aber dies hat sich geändert in zunehmende Integration und Vernetzung verschiedener Systeme und Speichertechnologien. »Dies bedeutet, dass IT-Administratoren ein immer breiteres Know-how über IT-Infrastruktur

benötigen«, meint Roth. »Sie müssen nicht nur tiefgehende Kenntnisse in spezifischen Speicherlösungen haben, sondern auch verstehen, wie diese Lösungen nahtlos mit anderen Komponenten der IT-Umgebung, wie Netzwerken, Servern und Anwendungen, zusammenarbeiten. Diese ganzheitliche Sichtweise ist entscheidend, um die steigenden Anforderungen an Effizienz, Flexibilität und Skalierbarkeit in modernen IT-Umgebungen zu erfüllen.«

»Interessant ist auch, wie Application-Owners, Data-Scientists oder Engineers mit Datenlösungen umgehen«, meint Netapp-Manager Kleff. »Sie erwarten nämlich, dass intelligente Lösungen ihnen die notwendigen Informationen für ihre Projekte automatisiert zur Verfügung stellen.« Netapp stellt dies beispielsweise mit APIs und Integration zum Beispiel in *Kubernetes*-Umgebungen sicher. Intelligente Datendienste sollen diesen Gruppen automatisierte Verwaltungsmöglichkeiten für containerbasierte Software-Architekturen zur Verfügung stellen. »Das ist nur ein Beispiel, aber es zeigt: Das sichere und zuverlässige Speichern von Daten, der Storage als Physik, spielt weiterhin eine zentrale Rolle im Unternehmen«, argumentiert Kleff. »Immer mehr in den Fokus rückt aber, diese Daten wo sie benötigt werden 'compliant' und automatisiert zur Verfügung zu stellen.« ■



Bild: via Canva pro



Peter Marvan
speicherguide.de



Karl Fröhlich
speicherguide.de

»Es gibt einfach keinen Grund mehr, HDDs zu kaufen« – oder doch?

FLASH VS. HDD: ARGUMENTE FÜR BEIDE TECHNOLOGIEN

Speicherkapazität, Geschwindigkeit und Kosten pro GByte waren bisher die Disziplinen in dem Dreikampf, den sich Flash-Storage und HDD-Storage lieferten. Die Flash-Fraktion räumt der Festplatte künftig keine Chancen mehr ein. Das HDD-Lager sieht dies selbstredend anders. Vielmehr könne Flash dem Datenwachstum nicht annähernd gerecht werden.

Viele vermeintlich längst abgeschriebene Technologien können sich noch lange erfolgreich halten – und für die Marktteilnehmer durchaus lukrativ sein. Gezeigt hat sich das kürzlich wieder einmal anhand der Zahlen für den Tape-Markt. Den **Technology Provider Companies** (TPCs) des LTO-Programms zufolge wurden 2023 LTO-Tapes mit einer Gesamtkapazität von rund 153 EByte ausgeliefert. Dies entspricht gegenüber dem Vorjahr einem Wachstum von drei Prozent. Für eine lange und oft totgesagte Technologie ist das recht ordentlich.

Seit einiger Zeit droht die Festplatte zumindest in der Wahrnehmung vieler Beobachter ein ähnliches Schicksal wie Tape. Die Technologie geriet bereits vor einigen Jahren durch den Siegeszug von Flash-Speicher unter Druck. Bislang verteidigte sie sich aber tapfer – auch wenn die Analysten von **Trendforce** berichteten, dass 2020 erstmals mehr SSDs (333 Millionen Stück) als HDDs (260 Millionen Stück) ausgeliefert wurden.

»Es gibt einfach keinen Grund mehr, HDDs zu kaufen«

Allmählich gehen jedoch der Festplatte die Ressourcen aus – auch wenn die Absatzzahlen im ersten Quartal 2024 das Gegenteil nahelegen. Das sieht zumindest **Rob Lee**, CTO von **Pure Storage**, so: »Es gibt einfach keinen Grund mehr, HDDs zu kaufen«,

sagte der Manager gegenüber *speicherguide.de*, während eines Besuchs in München. Und er fügte hinzu: »Sogar Tape ist da, wo es genutzt wird, besser. Und falls man Daten für 20 Jahre in einem Bergwerk speichern will, ist Tape sogar besser als Flash.«

Wer Pure kennt, der weiß, dass sich das Unternehmen seit seinem Bestehen für Flash-Storage stark gemacht hat. Parteilichkeit ist Lee deshalb nicht abzusprechen. Er führt für seine Ansicht aber viele nachvollziehbare Argumente ins Feld.

Zum einen sei die Festplatten-Technologie trotz immer wieder erstaunlicher und kaum noch erwarteter Fortschritte in den vergangenen Jahren nun da angelangt, wo sie vielleicht die physikalischen Grenzen noch nicht erreicht hat, in dem es aber immer schwerer wird, sich diesen Grenzen auch wirtschaftlich weiter anzunähern. Bei Flash profitiere dagegen auch der Enterprise-Bereich von der zunehmenden Verbreitung im Consumer-Bereich. Die Massenfertigung senke die Preise und erlaube den Produzenten viel Geld in die Verbesserung ihrer Prozesse und Technologien zu stecken. »Bereits jetzt bekommen Kunden im Enterprise-Umfeld Flash samt seinen Vorteilen zum selben Preis wie HDDs«, sagt Lee.

Als Damoklesschwert für Festplatten als Speichermedium im Rechenzentrum sieht Lee auch die Konzent-



Bild: Pure Storage

Rob Lee
CTO, Pure Storage

»Es gibt einfach keinen Grund mehr, HDDs zu kaufen«

ration des Marktes auf zwei Anbieter (**Seagate** und **Western Digital** – mit **Toshiba** als abgeschlagenem Dritten) und bei den Enterprise-Storage-Anbietern, die auf HDD setzen, auf sechs bis sieben. »Was passiert, wenn einer davon auf Flash umstellt«, fragte Lee – und gibt gleich selbst die Antwort: »Dann bricht der Markt dramatisch ein und setzt der stufenweise Niedergang ein.« Dass der Tag komme, sei aber unausweichlich – und letztlich die langfristige, schon von Anfang verfolgte Strategie von Pure gewesen.

Abgang auf Cold-Storage – wirklich?

»Cold-Storage hat sich auch überlebt«, schiebt Lee gleich eine weitere These nach. »Wenn ich schon dafür bezahle, dass ich Daten speichere, dann will ich sie auch nutzen«, sei die Devise im KI-Zeitalter. Noch stehe KI ganz am Anfang. Aber schon in naher Zukunft werde man Daten vor allem speichern, um sie zu nutzen.

»Die Erwartungen an Storage haben sich gewandelt«, betont Lee. Es gehe nicht mehr darum, Daten aufzubewahren (aus welchem Grund auch immer), sondern darum, sie regelmäßig zu nutzen. Da zudem das Datenwachstum rasch zunimmt, verlören ältere Daten relativ schnell an Bedeutung.

Zur Einordnung: Laut **IDC** betrug 2022 das weltweite Datenvolumen 103,66 ZByte, 2023 waren es 126,32 ZByte und 2024 sollen es 153,52 ZByte werden. Damit nähme das Datenvolumen alleine von 2022 bis 2024 um mehr als die 2019 insgesamt vorhandene Datenmenge (41 ZByte) zu.

Salopp gesagt, käme es bei diesem Zuwachs laut Lee auf die paar Altdaten, die auch noch im System liegen, schon nicht mehr an. Hohen Aufwand zu treiben, um sie in unterschiedlichen Storage-Tiers abzulegen, diese zu verwalten, das Backup dafür zu organisieren, die Integrität der Daten zu gewährleisten sowie die



Bild: Nimbus Data

Thomas Isakovich
CEO, Nimbus Data

»Festplatten werden dem Datenwachstum besser gerecht, als Flash-Speicher.«

Hardware-Infrastruktur zu pflegen, sei einfach eine Last. Auch deshalb ziehe Flash-Storage in Bezug auf die Gesamtbetriebskosten (TCO) an HDDs vorbei.

Nicht zuletzt hätten sich die Erwartungen an Storage geändert. Effizienz, Platzbedarf, Energiekosten für die Kühlung, die Zuverlässigkeit und der Betrieb der Storage-Umgebung insgesamt rückten immer mehr in den Vordergrund. Auch hier sieht Lee Flash gegenüber Festplatten insgesamt im Vorteil.

Huawei leistet mit SSD-Ankündigung Schützenhilfe

Schützenhilfe bei seiner Argumentation bekommt er indirekt von **Huawei**. Das Unternehmen hat auf seinem Innovative Datacenter Forum im Mai in Berlin nicht nur Tape als komplett überholt bezeichnet, sondern mit der *128 TB Huawei Palm-NVMe-SSD* einen Innovationssprung bei Flash-Storage vorgestellt. Der wird zwar voraussichtlich erst 2025 verfügbar sein, aktuelle Huawei-Systeme wie *OceanStor Dorado 3000* (All-Flash Storage der Einstiegsklasse für KMU) und *OceanStor Pacific 9950* (High-Density, High-Performance Distributed Storage) sind jedoch schon für die Unterstützung ausgelegt.

Die 128 TB Huawei Palm wird statt wie SSDs aktuell 15 nur noch 9,5 Mil-

limeter dick sein. Die Verschlüsselung auf dem Flash-Speicher soll so ausgestaltet sein, dass die Storage-Performance dadurch nicht beeinträchtigt wird und durch die hohe Dichte der NAND-Chips soll sich der Platzbedarf für ein System mit 1 PByte Speicherkapazität zu bisherigen Systemen um 88 Prozent und der Energiebedarf sogar um 92 Prozent reduzieren lassen. Die neu veröffentlichten SSDs bieten laut Huawei eine 10-mal höhere Kapazität bei gleicher Laufwerksgröße.

Das sei besonders nützlich für Datenzentren und Anwendungen, die große Mengen an Daten verarbeiten, wie zum Beispiel Big-Data-Analysen, Videobearbeitung und High-Performance-Computing. Durch die Verwendung der NVMe-Schnittstelle bietet die

SSD schnellere Datenübertragungsraten, niedrigere Latenzzeiten und höhere IOPS im Vergleich zu SATA-SSDs. Die Kombination von TLC- (Triple-Level Cell) und QLC-Flash-Technologie (Quad-Level Cell) hilft, die Balance zwischen Kosten, Leistung und Langlebigkeit zu erreichen. QLC ermöglicht es, mehr Daten pro Zelle zu speichern, was die Speicherdichte erhöht, während TLC eine höhere Schreibdauer und Zuverlässigkeit bietet.

Mit dem – bisher nur angekündigten – Produkt fordert Huawei jedoch die etablierten SSD-Anbieter heraus. Deren High-Capacity NVMe-SSDs liegen dagegen deutlich zurück. Die High-Capacity NVMe-SSDs von **Samsung** (etwa die Serien *PM1733* und *PM1735*) sind aktuell mit Kapazitäten bis zu 30,72 TByte verfügbar und nutzen die PCIe-4.0-Schnittstelle für schnelle Datenübertragungsraten. Bei Seagate ist zum Beispiel die *Nytra 3032 SAS-SSD*-Serie zu nennen, die bis zu 15 TByte mit SAS-Schnittstellen bietet, bei **Western Digital** die Serie *WD Gold*. Diese NVMe-SSDs erreichen Kapazitäten von bis zu 7,68 TByte.

Kein Grund die HDD für tot zu erklären

Eine komplett andere Meinung vertritt dagegen **Thomas Isakovich**, CEO und Gründer von **Nimbus Data** und prognostiziert: »Innerhalb von fünf Jahren werden keine neuen Pure Storage

Flash-Arrays mehr verkauft. Gründe sind überbeuerte und geschlossene Boxen mit unterdurchschnittlicher Leistung für das KI-Zeitalter sowie eine Erosion der Gewinnspanne, da sich SSD-Anbieter zunehmend bei der Dichte übertreffen. Hinzukommt ein nicht nachhaltiges Geschäftsmodell mit kumulierten GAAP-Verlusten in Höhe von über einer Milliarde US-Dollar seit der Gründung.« Für Isakovich sei dies eine viel wahrscheinlichere Behauptung als der prophezeite HDD-Tod.

Auch wenn die Aussage des Nimbus-Chef eher ironisch gemeint war, zog er sich natürlich direkt den Zorn des Pure-Lagers zu. Auf seinem LinkedIn-Account kam es weniger zu Diskussionen, als zu gegenseitigen Schuldzuweisungen.

Isakovich bezieht sich unter anderem auf gängige Fakten: Daten werden schneller generiert als je zuvor, und die Versuche, sie zu Geld zu machen, werde die Nachfrage nach Speicherplatz langfristig antreiben. Daher seien Stückzahlen ein schlechter Indikator für EByte-Trends, da die Laufwerkskapazität ständig steigt.

Während beispielsweise die HDD-Stückzahlen 2010 ihren Höhepunkt erreichten, stieg die ausgelieferte Festplatten-Kapazität zwischen 2018 (912 ausgelieferte EByte) und 2021 (1,35 ausgelieferte ZByte) um etwa 67,5 Prozent. Bis 2025 könnten, Marktforschern zufolge, weltweit mehr als 175



Bild: Huawei
Auf All-Flash-Speicher entfällt ein immer größerer Anteil im Rechenzentrum.

ZByte an Daten generiert werden. Die Storage-Branche bezweifelt, dass sich diese Datenmenge alleine mit Flash speichern lässt.

Der prognostizierte Kapazitätssprung ist teilweise auf das explosionsartige Wachstum des Internets der Dinge zurückzuführen. Laut **Fortune Business Insights** wird der IoT-Markt bis 2032 um mehr als das Fünffache seines derzeitigen Wertes wachsen. Eine weitere Rolle spielt die generative KI, die laut IDC-Prognosen die Nachfrage nach Datenspeichergeräten mit einer CAGR von bis zu 20 Prozent steigern soll.

Eine Studie von **Coughlin Associates** deutet darauf hin, dass die überwiegende Mehrheit der Daten noch für einige Zeit auf Festplatten gespeichert sein wird, auch wenn Flash-Speicher einen immer größeren Teil des Kuchens ausmachen werden. Für die drei wichtigsten Festplatten-Hersteller gibt es daher gute Gründe, die mittel- bis langfristigen Aussichten für Festplatten optimistisch zu sehen. ■

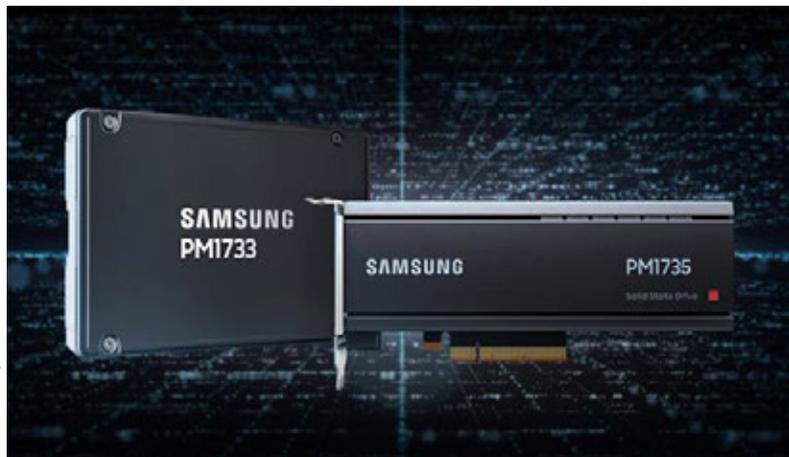


Bild: Samsung
Die High-Capacity NVMe-SSDs von Samsung PM1733 und PM1735 sind aktuell mit Kapazitäten bis zu 30,72 TByte verfügbar.



Actidata

actidata.com



Sitz der Gesellschaft:
Dortmund

Jahr der Gründung:
2009

Zielgruppe:
Systemhäuser, VARs und Industriekunden

Die actidata Storage Systems GmbH mit Sitz in Dortmund ist ein innovativer IT-Hersteller mit Schwerpunkten im Bereich Backup, Storage und Archivierung. Das Unternehmen konzentriert sich mit einem Netzwerk professioneller Systemhäusern auf das Industrie- und Geschäftskundensegment mit dem Ziel, professionelle Speicherlösungen zu platzieren.



N-TEC GmbH

n-tec.eu

Sitz der Gesellschaft:
Ismaning

Jahr der Gründung:
2001

Zielgruppe:
Vor allem KMU + öffentliche Auftraggeber

N-TEC konzentriert sich auf universell einsetzbare und skalierbare Speicherlösungen für Unternehmen und setzt dabei auf sorgfältig ausgewählte, namhafte Hersteller. Im Fokus stehen Object Storage Lösungen für Private Clouds und Storage Systeme mit hoher Verfügbarkeit. Klassische Server, SAN und Unified Storage Systeme, sowie revisions sichere WORM Archive und Backup Lösungen runden die Produktpalette ab. Kunden erhalten bei N-TEC alles aus einer Hand – vom Pre Sales bis zum After Sales und langjährigen Support. N-TEC ist immer der zentrale Ansprechpartner für alle Belange.



Holstein IT-Solutions

truenas.de/



Sitz der Gesellschaft:
Hagen

Jahr der Gründung:
2015

Zielgruppe:
mittelständische Industrieunternehmen, Behörden, Bildungseinrichtungen, Gesundheitswesen, Energiesektor, Mediendienstleister

Holstein IT-Solutions aus Norddeutschland vereint kompetente IT-Experten unter seinem Dach. Das junge und motivierte Team unterstützt Behörden, Bildungseinrichtungen sowie mittelständische und große Unternehmen bei Infrastrukturprojekten von der Planung über die Umsetzung bis hin zum Betrieb. Die Stärken sind Enterprise-grade Storage-, Security-, Netzwerk- und Virtualisierungslösungen. Der IT-Systemspezialist setzt bevorzugt auf Open Source sowie offene Standards für mehr Kompatibilität und Investitionsschutz.



FAST LTA

www.fast-lta.de



Sitz der Gesellschaft:
München

Jahr der Gründung:
1999

Zielgruppe:
KMUs, VARs und Industriekunden

Wir sind die Spezialisten für Sekundärspeicher, für Archivierung und Backup.

Unsere Produkte und Services helfen mittelständischen Anwendern, Datensicherung und Datenmigration zu vereinfachen, rechtliche und regulatorische Risiken zu minimieren, und das langfristige Risiko, Daten zu verlieren, nachhaltig zu verringern.

LTO-Tape-Libraries und LTO-Tape Streamer in virtuellen Umgebungen einsetzen

ACTIDATA T-PONTIS – JETZT WIRD »GEBRIDGED«

Das iSCSI-Protokoll ermöglicht über 10Gb-Ethernet eine effiziente und kostengünstige Verwaltung von LTO-Tape-Libraries. Die 10GbE-iSCSI-Bridge actidata T-Pontis unterstützt bis zu vier LTO-Laufwerke zu betreiben, unabhängig von zentralen Betriebssystemen, in virtuellen Umgebungen sowie an einem entfernten Standort.

Die Nutzung des iSCSI-Protokolls über 10Gb-Ethernet bietet eine einfache und kostengünstige Lösung für die Verwaltung und den Betrieb von LTO-Tape-Libraries sowohl direkt im Rechenzentrum als auch in einem entfernt installierten IT-Rack. Die **actidata T-Pontis 10GbE-iSCSI-Bridge** bietet hier die nötigen Leistungsmerkmale. Mit zwei optischen 10Gb-Ethernet-Schnittstellen können bis zu vier LTO-Laufwerke, eingebaut in einer LTO-Tape-Library sowohl von einem dedizierten Backup- & Archiv-Server, als auch direkt aus einer virtuellen Maschine (VM) heraus betrieben werden. Dank iSCSI agiert die **actidata T-Pontis 1U-Bi** unabhängig von zentralen Betriebssystemen und wird über einen iSCSI-Initiator direkt angesteuert.

actidata T-Pontis 1U-LTO mit eingebautem LTO-Laufwerk

Ganz besonders für die Erstellung zusätzlicher Datensicherungen neben



Bild: actidata

actidata T-Pontis 1U-Bi als 10GbE-to-SAS-Bridge & T-Pontis 1U-LTO mit eingebautem LTO-Laufwerk.

NAS- und Cloud-Backups empfiehlt sich der Einsatz des **actidata T-Pontis 1U-LTO-Systems**. Hierbei ergänzt ein eingebauter LTO-Streamer die 10GbE-Bridge in einem 1U-Rackmount-Gehäuse, das vorzugsweise an einem entfernten Standort (Stichwort: 2. Brandabschnitt) installiert und über vorhandene Ethernet-Topologien betrieben wird.

Anzeigen an der Vorderseite

Übersichtlich dargestellt: An der Vorderseite der actidata T-Pontis 1U-Sys-

beleuchtete Taster auch gleich den Betriebszustand anzeigt.

Informationen zur actidata T-Pontis Produktfamilie anfordern

Neben der 10GbE-iSCSI-Bridge actidata T-Pontis 1U-Bi in einem robusten 1U-Rackmount-Gehäuse steht diese auch mit einem eingebautem LTO-Laufwerk zur Verfügung. Das actidata T-Pontis 1U-LTO ist wahlweise mit einem LTO-8- oder einem LTO-9-Laufwerk ausgestattet. Die empfohlenen Netto-Einkaufspreise für den Anwender starten bei zirka 4.900 Euro. ■

Weitere Informationen:

actidata Storage Systems GmbH

Wulfshofstr. 16 – Indu-Park
44149 Dortmund
Tel. 0231/96 36 32-0
E-Mail: info@actidata.com
www.actidata.com



Albrecht Hestermann
actidata Storage
Systems

5 Maßnahmen für eine sichere Geschäftskontinuität

OHNE DATEN KEIN GESCHÄFT

Für ihre Geschäftskontinuität benötigen Unternehmen einen Plan, auch Mittelständler. Im Krisenfall sind schnelle und effektive Maßnahmen entscheidend, um schwerwiegende Geschäftsauswirkungen zu vermeiden. Dabei sind effiziente Backups und durchdachte Disaster-Recovery-Prozesse unerlässlich für die schnelle Wiederherstellung und Verfügbarkeit kritischer Daten.



Benedict Schultz
Holstein IT-Solutions

Im Krisenfall zählt jede Minute. Je länger auf Daten nicht zugegriffen werden kann, desto drastischer sind die Auswirkungen für das Geschäft. In komplexen IT-Umgebungen sind geschäftskritische Daten oft über mehrere Instanzen, Cloud-Dienste und SaaS-Plattformen verteilt. Ein praxistauglicher Plan, funktionierende Backups und routinierte Disaster-Recovery-Prozesse helfen im Ernstfall, das Schlimmste zu verhindern. In diesem Artikel geben wir Tipps für ein erfolgreiches Business-Continuity-Programm und die schnelle Wiederverfügbarkeit von Daten im Katastrophenfall.

Fünf Maßnahmen für ein unterbrechungsfreies Geschäft ohne Datenverlust

Katastrophen sind unterschiedlicher Natur. Nicht immer sind es Ransomware-Angriffe, welche den Datenbestand eines Unternehmens gefährden. Viel häufiger führen Hardware-Ausfälle,

Bedienfehler, Fehlkonfigurationen oder das versehentliche Löschen ganzer Datensätze zu einem Problem. Auch physische Ursachen wie Feuer, ein Rohrbruch oder eine Naturkatastrophe können zu Unterbrechungen und dem Verlust wertvoller Daten führen. Ein Geschäftskontinuitätsplan hilft, die Auswirkungen einzudämmen. Zwei Kennzahlen sind dabei relevant: RTO und RPO. RTO meint die Zeit bis zur Wiederherstellung eines Systems oder Datensatzes (Recovery Time Objective). Wie viele Daten verloren sind, besagt der RPO-Wert (Recovery Point Objective). Erstrebenswert ist in beiden Fällen eine Zahl möglichst nahe an Null. Weder möchte ein Unternehmen zu viele Daten noch zu viel Zeit bei der Wiederherstellung verlieren. Mit ein paar Maßnahmen werden Unternehmer ihrer Verantwortung gerecht und müssen keine Angst vor einer Katastrophe haben. Die wichtigsten Maßnahmen sind:

1. Kontinuierliche Datensicherung

Die kontinuierliche Sicherung von Daten ermöglicht eine Wiederherstellung zu jedem beliebigen Zeitpunkt. Das Backup sollte mehrstufig sein und der 3-2-1-Regel folgen. Dabei werden drei Kopien angefertigt, welche auf mindestens zwei unterschiedlichen Medien gespeichert werden. Eines der Medien sollte offline vorgehalten werden. Initial sollte immer ein Voll-Backup gemacht werden. Anschließend werden Daten inkrementell gesichert. Das heißt, nur die Veränderungen werden aufgezeichnet. Auf diese Weise werden wichtige Ressourcen wie Platz, Zeit und Bandbreite gespart. Offline-Speicherorte können ein Tresor (physischer Air-Gap) oder auch ein sicherer Cloud-Speicher (virtual Air-Gap) sein. Beim Tresor ist wichtig, dass er sich mindestens in einem anderen Brandabschnitt wie die Originaldaten befindet. Noch besser sind auf die sichere Aufbewahrung sensib-

ler Daten spezialisierte Dienstleister. Unsere Empfehlung sind zusätzliche Snapshots für eine schnelle Wiederherstellung. Außerdem raten wir dazu, auch Abbilder (Images) von Servern und virtuellen Maschinen zu sichern. Auf diese Weise kann ein ganzer Standort innerhalb kürzester Zeit wiederhergestellt werden.

2. Ausfallsicherheit

Die größte Katastrophe ist sicher, wenn ein ganzer Standort ausfällt. Aber auch kleine Vorfälle – wie der Ausfall von Speichermedien oder eines Netzteiltes – können eine große Auswirkung haben. Kleineren Katastrophen wie dem Ausfall einer Platte oder eines Netzteiltes kann einfach vorgebeugt werden. RAID-Konfigurationen auch innerhalb eines Systems verschmerzen den Ausfall einer oder sogar mehrerer HDDs oder SSDs. Wichtige Bauteile wie Controller oder Netzteile sollten immer redundant

vorhanden sein und bei Ausfall einer Komponente die volle Last stemmen können. Kritische Geschäftsdaten sollten zudem geo-redundant, das heißt, an mindestens zwei unterschiedlichen Orten vorgehalten werden. Im Cloud-Zeitalter ist das auch kein Problem mehr. Es gibt ausreichend europäische und deutsche Anbieter, welche auch für die Speicherung sensibler Daten kein Risiko darstellen. Mit den gesicherten Images von Servern und virtuellen Maschinen kann die Cloud auch als Disaster-Recovery-Standort fungieren. Selbst wenn man den primären Standort nicht als Spiegel an einem zweiten Standort oder in der Cloud betreibt, lassen sich Dienste innerhalb kürzester Zeit wiederherstellen, und die Arbeit kann fortgesetzt werden. Das verschafft Unternehmen ausreichend Zeit für die Wiederherstellung der primären Ressourcen und Dienste.

3. SaaS & Cloud ins Backup einbeziehen

Immer öfter werden Daten bei Anbietern von Software as a Service (SaaS) gespeichert. *Microsoft 365* oder CRM-Dienstleister wie *HubSpot* oder *Salesforce* sind die bekanntesten Dienste. Aber nicht nur SaaS-Daten können manipuliert werden oder verloren gehen. Das gleiche gilt auch für Daten in Cloud-Services. Was viele Unternehmen oft nicht wissen: SaaS- oder



TrueNAS-Enterprise-Appliances sind hochverfügbare Komplettlösungen für Datensicherung und Disaster Recovery in Behörden, Unternehmen oder Schulen.

Cloud-Service-Provider garantieren zwar die Verfügbarkeit der Daten (Durability), nicht aber die Integrität. Auch Daten bei Service-Providern können das Ziel von Angriffen sein oder Opfer eines Bedienfehlers werden. Daher ist es wichtig, auch diese Daten in die Backup-Strategie einzubeziehen. Viele Backup-Lösungen eignen sich inzwischen für das Sichern von Cloud- und SaaS-Daten. Quelloffene Produkte verhindern ein sogenanntes Vendor-bzw. in diesem Fall Daten-Lock-in.

4. Schutz vor Manipulation

Daten sind vielfältigen Gefahren ausgesetzt: mutwillige oder versehentliche Manipulation bzw. Löschung, Schreibfehler aufgrund von Netzwerkproblemen oder defekter Hardware und Bitrot. Damit es bei einer Wiederherstellung im Störfall nicht zu bösen Überraschungen kommt, sollten sowohl die Übertragung als auch die

Integrität der Daten lückenlos überwacht werden. Dabei helfen Prüfsummen (Checksums) und die Analyse der Datenströme. Auf diese Weise können Manipulationen bereits in einem sehr frühen Stadium erkannt und Maßnahmen ergriffen werden. Aber auch andere Maßnahmen helfen beim Schutz unternehmenskritischer Daten. So regelt ein Rollen- und Berechtigungskonzept, wer welchen Zugang zu und Zugriff auf Daten hat. Zentrale Verzeichnisdienste helfen bei der Durchsetzung dieser Regeln. Netzwerküberwachung hilft bei der Angriffserkennung; unberechtigte Zugriffe können rechtzeitig wirksam verhindert werden. Eine mehrstufige Sicherheitsarchitektur birgt zusätzliche Barrieren für Angreifer von außen wie von innen. Maßnahmen wie Allow-Listing und das Einschränken von Rechten auf bestimmte Ressourcen wie die Backup-Daten bieten zusätzliche Sicherheit.

5. Testen! Testen! Testen!

Das Backup von Daten lässt sich leicht automatisieren. Dabei können sich jedoch mit der Zeit Fehler einschleichen. Umso wichtiger ist es, die Integrität der Backup-Daten regelmäßig zu überprüfen. Auch die Wiederherstellung sollte für den Ernstfall regelmäßig geprobt werden. Auf diese Weise zeigen sich auch Schwachstellen im Prozess – der Prozess kann insgesamt optimiert werden. Einige Lösungen bieten integrierte – simulierte – Wiederherstellungstests an. Wir empfehlen dennoch mindestens einmal im Jahr eine praktische Übung zur Wiederherstellung im Katastrophenfall durchzuführen. Anders als bei einer Simulation wird dabei auch geprobt, dass jeder Mitarbeiter weiß, was zu tun ist und ob die Zuständigkeiten klar definiert sind. Unser Pro-Tipp: Drucken Sie Notfallpläne und Notrufnummern auf Papier aus. Wenn

die IT ausfällt, ist auch der Zugriff auf elektronische Dateien futsch.

Fazit: Begegnen Sie Risiken mit einem konsequenten Plan

Die Datenmenge wächst rasant und der Schutz dieser Daten wird immer anspruchsvoller. Eine krisensichere IT-Landschaft und integre Daten sind jedoch kein Hexenwerk. Mit ein paar Maßnahmen ist Ihr Unternehmen vor dem Größten geschützt. Wichtig sind drei Dinge:

- Kennen Sie Ihre Risiken.
 - Machen Sie einen Plan.
 - Setzen Sie den Plan konsequent um.
- So bleiben wichtige Daten geschützt und Ihr Unternehmen geschäftsfähig. Fehlen Ihnen Wissen oder Ressourcen inhouse, bitten Sie einen Partner Ihres Vertrauens um Unterstützung. Systemhäuser wie **Holstein IT-Solutions** unterstützen kleine und große Unternehmen von der Konzeption über die Umsetzung bis hin zum Betrieb. Das Team von Holstein IT-Solutions liefert auch schlüsselfertige Komplettlösungen auf Basis von Open-Source und offenen Standards. ■

Weitere Informationen:

Holstein IT-Solutions

Dorfstraße 18a
24576 Hagen
Tel. 04822/30 35 210
E-Mail: truenas@holstein-it-solutions.de
www.holstein-it-solutions.de

SAN-Speicher zum Volkspreis

AB AUF DIE ÜBERHOLSPUR: 10 GRÜNDE FÜR NVME-SANS IM MITTELSTAND

I/O-hungrige Applikationen wie konkurrierende Datenbanken und Virtualisierung, KI und Analyse, Machine-Learning und Edge – sie alle erfordern heute die Performance, Sicherheit und Verfügbarkeit eines lokalen All-Flash-SANs. State-of-the-Art sind zweifellos NVMe-Speicher. Das gilt auch für KMU und Mittelstand.

State-of-the-Art klingt schön und gut. Die Leistungsanforderungen genannter I/O- und Latenz-empfindlichen Applikationen erfordern eine Block-Speicherlösung, mit Ausfallsicherheit durch physische Redundanz und die Geschwindigkeit einer lokale SAN-Lösung. NAS- und Cloud-Konzepte sind dafür kaum geeignet. Die Krux für KMU und Mittelstand: Wie bezahlbar sind solche Lösungen? Wie handhabbar, ohne große IT-Abteilung?

Dabei ist SAN nicht gleich SAN. Lösungen unterscheiden sich in Medium und Transferprotokoll. Verbreitet sind bis heute, aus historisch gewachsenen oder vordergründig finanziellen (Anschaffungs-)Gründen, Fibre-Channel- und kostengünstigere iSCSI-SANs. Sie arbeiten mit SAS-SSD, drehenden HDD-Spindeln oder in hybrider Ausführung. FC-over-Ethernet (FCoE) kann als Protokollvariante angeführt werden. Auch



NVMe unterstützt durch parallele Datenverarbeitung über die PCIe-Lanes 64.000 Befehle pro Warteschlange, SAS nur bis zu 256 Befehle.

eine hyperkonvergente Infrastruktur (HCI) oder paralleles NFS können Block-Level Speicherdienste liefern. Aber kaum für KI und Konsorten.

Quantensprung: NVMe ist der Turbo für SANs

NVMe macht zu diesen SAN-Optionen einen echten Unterschied. NVMe kommuniziert direkt mit dem PCIe-Bus (Peripheral Component Interconnect Express) und benötigt nicht den Um-

weg über CPU und HBAs wie SATA. Dabei unterstützt NVMe durch parallele Datenverarbeitung über die PCIe-Lanes 64.000 Befehle pro Warteschlange. Zum Vergleich: SAS unterstützt nur bis zu 256 Befehle pro Warteschlange, SATA bis zu 32.

Effekt sind kürzere Latenzen um etwa den Faktor vier im Bereich von etwa 30 Mikrosekunden und entsprechender Leistung von über 500.000 IOPS (Input/Output Operations per

Second) pro Modul. Mit NVMe-over-Fabrics (NVMe-oF) können zudem Architekturen über Netzwerkverbindungen hinaus skaliert werden. Und schlussendlich sind NVMe-Medien energieeffizienter als Vorgänger-SSDs.

Die Fakten verdeutlichen, dass NVMe in Bezug auf die Leistung ein echter Quantensprung ist. Entscheidend ist dabei, was dies in der Praxis bedeutet: Bessere Performance geht einher mit deutlich weniger Ressourcen, weniger Energieaufwand, weniger Lifecycle-Management für Medien, einfacheres Handling und weiteres. Letztlich steht NVMe für Kosteneinsparung und Investitionssicherheit, auch und gerade für KMU und Mittelstand.

Für IT-Manager von kleinen und mittleren Unternehmen haben wir zehn Argumente für den Einsatz im Mittelstand erfasst.



Sven Meyerhofer
N-TEC

Von der Theorie zur Praxis: 10 Gründe für NVMe im Mittelstand

1. Datenbanken: Mittelständische Unternehmen nutzen häufig ERP-Systeme, CRM-Software und SQL, NoSQL und In-Memory-Datenbanken. NVMe-SANs bieten die nötige Leistung, um diese Anwendungen effizienter und zuverlässiger zu betreiben, was auch zu verbesserten Benutzererfahrungen führt.

2. Virtualisierung und Cloud: Viele mittelständische Unternehmen setzen auf Virtualisierungstechnologien und hybride Cloud-Modelle, um ihre IT-Infrastruktur zu optimieren und Kosten zu senken. NVMe-SANs verbessern die Performance von virtuellen Maschinen und Containern erheblich, was die Effizienz und Skalierbarkeit der IT-Umgebung erhöht.

3. Schnellere Datenanalysen: Mittelständische Unternehmen profitieren von schnellen Datenanalysen, um fundierte Geschäftsentscheidungen zu treffen. NVMe-SANs ermöglichen schnellere Verarbeitung großer Datenmengen, was die Effizienz von Business-Intelligence (BI) und Analyse-Tools verbessert.

4. KI- und ML-Modelle erfordern schnelle und kontinuierliche Datenzugriffe für Training und Inferenz. NVMe-SANs bieten die erforderliche Performance, um diese Prozesse zu beschleunigen.

5. Content-Delivery und Medien-Streaming benötigen schnellen und zuverlässigen Zugriff auf große Mediendateien. NVMe-SANs können die erforderliche Bandbreite und Leistung bereitstellen, um ein reibungsloses Benutzererlebnis zu gewährleisten.

6. High-Performance-Computing (HPC): NVMe-SANs sind ideal für HPC-Umgebungen, in denen extrem niedrige Latenz und hohe IOPS erforderlich sind, um große Datenmengen schnell zu verarbeiten.

7. Kosteneffizienz durch bessere Ressourcennutzung: Obwohl NVMe-basierte Lösungen zunächst teurer erscheinen, bieten sie langfristig Kostenvorteile durch eine effizientere Ressourcennutzung. Die hohe Performance von NVMe-SANs bedeutet, dass weniger Hardware benötigt wird, um die gleichen oder bessere Ergebnisse zu erzielen, was die Gesamtkosten für Strom, Kühlung und Wartung reduziert.

8. Verbesserte Benutzererfahrung: In Bereichen wie E-Commerce und Kundenservice, in denen schnelle Reaktionszeiten entscheidend sind, sorgen NVMe-SANs für eine verbesserte Benutzererfahrung durch schnelle Datenzugriffe und reduzierte Latenzzeiten.

9. Skalierbarkeit und Zukunftssicherheit: Die schnelle Datenverarbeitung und -zugriffszeiten von NVMe-SANs sind entscheidend für die effiziente

Nutzung neuer Technologien. Sie bieten dabei eine hohe Skalierbarkeit, was es mittelständischen Unternehmen ermöglicht, ihre Speicherinfrastruktur flexibel an wachsende Anforderungen anzupassen.

10. Einfache Integration und Verwaltung: Moderne NVMe-SAN-Lösungen bieten oft benutzerfreundliche Management-Tools, die die Integration und Verwaltung der Speicherinfrastruktur vereinfachen. Dies ist beson-



Die QSAN-Speicher basieren auf einer offenen Architektur ohne Vendor-Lock-in.

ders für mittelständische Unternehmen wichtig, die möglicherweise nicht über umfangreiche IT-Ressourcen verfügen.

Für mittelständische Unternehmen sind NVMe-SANs eine lohnende Investition, um die IT-Infrastruktur zu modernisieren und die Leistungsfähigkeit zu steigern. Dies ermöglicht es mittelständischen Unternehmen, wettbewerbsfähig zu bleiben und auf zukünftige Herausforderungen vorbereitet zu sein.

Die Rolle eines lokalen Partners: NVMe zum »Volkspreis«

KMU und Mittelstand haben branchenübergreifend besondere Anforderungen: Diese sind zum einen die experimentfreie Implementierung einer maßgeschneiderten zugeschnittenen Lösung, ein zuverlässiger Support vor Ort und letztlich natürlich der Preis. Das **N-TEC**-Angebot deckt genau diese Anforderungen ab.

Individuelle Speicherlösungen sind unser Fachgebiet. Wir erfassen in ausführlichen Beratungsgesprächen den Bedarf eines Unternehmens vor Ort und stellen den entsprechenden All-Flash-Storage zusammen. Dabei profitieren gerade Mittelständler von unserer langjährigen Erfahrung rund um Storages und hochverfügbare Server.

N-Tec setzt bei ihren All-Flash-Speicherlösungen auf die zuverlässige Hardware von **QSAN**, deren Hardware auf offener Architektur ohne Vendor-Lock-in aufbauen und so variabel mit weiteren Hard- und Software-Komponenten kombiniert werden können. Durch die Expertise des lokalen Dienstleisters können so preisgünstige Gesamt-Pakete assembliert werden, die im Mittelstand eher greifen als jene globaler Anbieter. So ist zumindest das Konzept.

Basis des NVMe-SAN-Angebots von N-Tec ist das System **QSAN XCubeFAS XF3126D**. Es handelt sich um ein kom-

paktes 3U-System mit dualen, XEON-getriebenen Controllern, bis zu 384 GByte Memory pro Controller und knapp 400 TByte Kapazität (mit 15 TByte SSDs) aus 26 NVMe-Laufwerk-Slots.

Die enthaltene **QSAN XEVO**-Software erledigt Active-Active-Hochverfügbarkeit, Deduplizierung, Thin-Provisioning, Kompression, Snapshots, Volume-Clones, RAID, Verschlüsselung sowie API-Anbindung und -Unterstützung. Über remote stationierte Systeme und asynchrone Spiegelung kann zusätzliche Datensicherheit implementiert werden.

Das **QSAN XCube FAS NVMe** ist durch seine Leistung, Zuverlässigkeit und Skalierbarkeit sicher mehr als ein Einstieg in die NVMe-Welt. Häufig sind mittelständische Kunden aber überrascht, dass sie sich ein NVMe-SAN überhaupt leisten können. Die Preise liegen bei unter 20.000 Euro. Wir bei N-Tec verstehen wir dies augenzwinkernd unter Volkspreis.

N-Tec bietet das **QSAN XCubeFAS XF3126D** mit 23 TByte (6x 3,84 TByte) brutto derzeit zum Aktions-Endkundenpreis von 19.999 Euro an. ■

Weitere Informationen:

N-Tec GmbH

Adalperostrasse 29
D-85737 Ismaning
Tel. + 49 (0) 89 - 95 84 07-0
www.n-tec.eu/

Kleinere, schnellere, günstigere Backups

SILENT BRICKS MIT FAST CLONE SUPPORT FÜR VEEAM

Eine schnelle und vollständige Wiederherstellung der Daten ist im Fall eines Cyberangriffs essenziell. All-Flash-Storage löst dabei nur Teilbereiche und treibt die Kosten zusätzlich in die Höhe. Effizienter sind Software-Technologien, die im Primary- und Secondary-Target die benötigte Zeit um bis zu 80 Prozent und den erforderlichen Speicherbedarf um bis zu 50 Prozent reduzieren.



Hannes Heckel
FAST LTA

Zur Absicherung vor den Folgen eines Cyberangriffs sind Backups nach wie vor das Mittel der Wahl. Um nach einer erfolgten Attacke Daten so schnell wie möglich wieder vollständig herstellen zu können, werden Datenbereiche in verschiedene Klassen unterteilt, die mit unterschiedlichen Parametern zu einer Gesamtstrategie beitragen. Es entstehen Backup-Instanzen zur schnellen Verfügbarkeit, zur vollständigen Absicherung über längere Zeiträume sowie als »Last Line of Defense« mit ausgelagerten Datensätzen. Dabei gilt es für die einzelnen Instanzen zu bewerten, wie die Parameter Performance, Kapazität und Skalierbarkeit, Sicherheit und Kosten in konkrete Konfigurationen und Technologien umzusetzen sind.

Obwohl es sicher wünschenswert wäre, die gesamte Datensicherung in kürzesten Abständen für lange Zeit-

räume mit mehreren Instanzen und höchster Absicherung auf All-Flash-Storage zu bewerkstelligen, dürfte in den meisten Fällen das Budget der limitierende Faktor dafür sein. Es gehört zur »Best Practice«, die eingesetzten Technologien nach den einzelnen Instanzen zu staffeln und so Kosten zu sparen.

Primary Target – Geschwindigkeit ist alles.

Die erste Backup-Instanz dient dazu, Daten so schnell wie möglich wieder bereitstellen zu können. Hier kommt man um Flash-Storage kaum herum. Da dieser Bereich dadurch mit steigendem Speicherbedarf sofort sehr viel höhere Kosten verursacht, wirkt sich der Umstieg auf *Forever Incremental* mit *Fast Clone*-Support unmittelbar finanziell aus. 30 bis 40 Prozent Speicherplatz lassen sich so einspa-

ren – oder für längere Sicherungszeiträume nutzen. Auch die deutliche Performance-Steigerung nimmt man im Primary-Target gerne mit – je schneller, desto besser. Mit dem Flash-basierten *Silent Brick Plus* bietet das Silent-Brick-System dafür das ideale Speichermedium.

Secondary Target – Langfristig abgesichert.

Per Backup-Copy werden die Daten aus der ersten Instanz regelmäßig auf das zweite Backup-Ziel kopiert und über einen längeren Zeitraum gespeichert. Dabei kommt es nicht unbedingt auf maximale Performance, sondern auf höchste Sicherheit gegen Manipulation und Löschen sowie auf das beste Verhältnis von Kapazität zu Kosten an. Der *Silent Brick Max* mit seinen robusten 3,5-Zoll-Festplatten lässt sich dafür kostengünstig und in

Der neue Silent Brick Plus enthält zwölf schnelle SSDs und eignet sich ideal als Primary Backup Target mit Fast Clone Support.

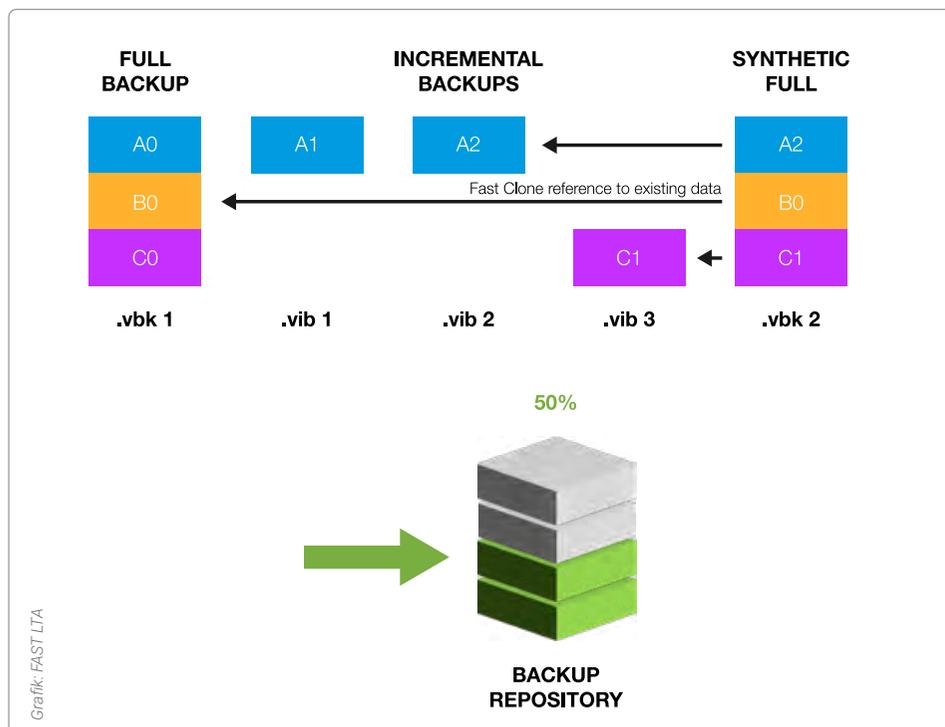


Grafik: FAST LTA

großen Kapazitäten erweitern. Im Secondary Target wirkt sich die Einsparung im Speicherplatz durch die häufigen Full-Backups noch dramatischer aus. 50 bis 70 Prozent weniger Speicherplatz sind je nach Konfiguration und Anwendung keine Seltenheit.

Air-Gap – Die Last Line of Defense

Sollten beide Erstinstanzen den Restore versagen, muss auf separate Sicherungen zurückgegriffen werden, die sich außerhalb des eigentlichen Speichersystems befinden. Je nach



Definition ist der Air-Gap dabei tatsächlich wörtlich oder eher im übertragenen Sinne zu verstehen. Eine einfache Trennung von Netzen – auch als »virtual Air-Gap« bezeichnet – stellt in den seltensten Fällen eine wirkliche Hürde für versierte Angreifer dar, wenn diese bereits in der Lage waren, die vorgelagerten Backups unbrauchbar zu machen. Air-Gaps sollten also am besten physisch erfolgen. Ideal sind Full-Backups auf dem *Silent Brick Air*, der sich aus dem System herausnehmen lässt.

Immutability – Doppelt hält besser.

Dass Backups besonderen Schutz erfordern, dürfte sich herumgesprochen haben: Fast jeder Angriff zielt inzwischen darauf ab, zunächst die Datensicherung unbrauchbar zu machen. Deshalb müssen Backups vor Manipulation und unerlaubtem Löschen geschützt werden. Um dies zu erreichen, setzen spezialisierte Speichersysteme wie das Silent-Brick-System Technologien ein, die fest verankert und von der Backup-Software unabhängig sind. Das Stichwort dafür heißt

Immutability, also die unveränderbare Speicherung. Anders als in der Archivierung wird die Unveränderlichkeit dabei auf einen bestimmten Zeitraum begrenzt, die so genannte Retention. Innerhalb der Retention kann kein Dienst oder User Daten verändern oder löschen. Im Silent-Brick-System geschieht dies über *Continuous Snapshots*, die in regelmäßigen Abständen den genauen Zustand des Dateisystems sichern. Bei Veränderung der Originaldaten werden diese durch die Snapshot-Logik separat gesichert, so

dass man jederzeit zu den vorherigen Zuständen zurückkehren kann.

Immutability erbt vom Backup aber dessen Problematiken: Je mehr Snapshots erzeugt werden und je länger die Retention, desto mehr Speicherplatz wird benötigt – und desto länger dauert der Prozess.

Fast Clone Support minimiert jedoch auch bei Continuous-Snapshots Speicherplatzbedarf und Aufwand. Durch den Einsatz von Synthetic-Full-Backups ist die sich verändernde Datenmenge sehr viel geringer, was sich 1:1 auch auf die Continuous-Snapshots auswirkt. Statt ganze Active-Full-Backups aufbewahren zu müssen, werden nur noch die Teile vor dem Löschen gesichert, die sich im Synthetic-Full tatsächlich verändert haben.

Fazit: Fast Clone Support ist ein bisschen magisch.

Es klingt ein bisschen magisch und ist doch so logisch: Statt dieselben Daten immer und immer wieder abzuspeichern und so zu vervielfachen, sorgt Fast Clone Support dafür, dass bereits vorhandene Daten in der Folge nur noch referenziert werden.

Dies hat dramatisch geringeren Speicherplatzbedarf und sehr viel kürzere Backup-Zeiten zur Folge. Im Primary-Target werden Forever-Incremental-Backups auf dem All-Flash Silent Brick Plus schneller und kleiner. Noch mehr wirkt sich die Unterstüt-

zung für Fast Clone im Secondary Target auf Silent Brick Max aus. Statt vieler Active-Full-Backups, die zusätzlich noch durch Immutability abgesichert werden müssen, kommen Synthetic-Fulls zum Einsatz. Hier lassen sich Einsparungen von 50 Prozent und mehr erreichen.

Das Silent Brick System ist das erste Speichersystem auf Linux-Basis, das Fast Clone Support direkt auf dem sicheren Dateisystem ZFS (im Silent Brick System *SecureNAS* genannt) und SMB-Shares realisiert und so keine komplexe und potenziell unsichere zusätzliche SSH-Verbindung zur Konfiguration benötigt.

Wie man durch frühzeitiges Auslagern unstrukturierter Daten das Backup noch einmal verschlanken kann, haben wir in diesem Hintergrund-Artikel beschrieben: <https://hallo.fast-lta.de/weniger-backup-mehr-sicherheit>

Mehr Informationen zum Fast Clone Support für Silent Bricks erhalten Sie hier: <https://www.fast-lta.de/de/thema/fast-clone-support> ■

Weitere Informationen:

FAST LTA GmbH

Rüdesheimer Str. 11,
80686 München
Tel. 089/89 047-0
E-Mail: info@fast-lta.de
www.fast-lta.de

Mit mehr als 250Mbyte/s auf ein austauschbares Medium sichern

ACTIDATA DX6-PRODUKTFAMILIE – EINFACH MAL BACKUP MACHEN

Die Anforderungen an Datenverfügbarkeit und Betriebssicherheit sind auch in kleinen und mittleren IT-Umgebungen geschäftskritisch. Lösungen müssen aber ins Budget passen und dürfen auch nicht zu komplex sein. Actidata positioniert sich hier mit seiner DX6-Serie, die sowohl als ein NAS- als auch ein Backup-System agieren.



Albrecht Hestermann
actidata Storage
Systems

Mit einer hohen Performance auf ein austauschbares Medium zu sichern – das war die Herausforderung, die sich die **actidata** bei Konzeption und Umsetzung einer neuen Produktlinie gestellt hat. Es galt, eine Alternative für die externe Datensicherung und Archivierung zu schaffen, die insbesondere in kleinen und mittleren IT-Umgebungen den Anforderungen an Datenverfügbarkeit und Betriebssicherheit erfüllen. Hierbei spielt das Backup auf austauschbare Medien die entscheidende Rolle, denn die externe Lagerung der Datensicherungsätze gilt als letzte Bastion im Rahmen eines Cyber-Security-Konzeptes.



Bild: actidata

actidata DX6-Desktop-Variante Q-DX6 und Qx-DX6.

Mit mehr als 250 MByte/s auf Wechselfestplatten sichern

Mit der Bereitstellung der *actidata DX6*-Produktfamilie werden die gesetzten Performance-Ziele erreicht. Durch Optimierung der Hardware und durch Anpassung der eingesetzten Betriebssysteme und Tools werden

die Leistungsmerkmale der hochkapazitiven 3,5-Zoll-Festplatten bestens ausgenutzt. Konkret: Die Datenströme sind intern mit mehr als 250 MByte/s realisiert. Dies entspricht durchaus einem Faktor von 2 bis 2,5 im Vergleich zu handelsüblichen 2,5-Zoll-Festplatten. Somit lassen sich Daten-

sicherungen, die typischerweise im KMU-Bereich anfallen, locker über die Nacht oder das Wochenende auf ein austauschbares Medium übertragen. Diese stehen aktuell mit jeweils 4, 8, 12, 16 und 20 TByte bereit.

DX6-Systeme mit Windows Server IoT als offenes System

Sowohl die Desktop-Variante *actidata Q-DX6* als auch die 2U-Rackmount-Version *RM-DX6* setzen auf die CAL-free Version vom *Windows Server IoT*. Beide Systeme stellen über SMB-Freigaben den Produkktivsystemen NAS-Speicher für das Disk-basierende Backup zur Verfügung – beim *RM-DX6*



Bild: actidata

*actidata RM-DX6
und RMx-DX6 als 2U
Rackmount-Variante*

sogar mit eingebautem RAID-Controller. Eine Backup-Software für die Datensicherung wird seitens actidata nicht vorgegeben, so dass der Anwender in eigener Regie die bevorzugte Windows-basierende Applikation installieren und betreiben kann. Selbstverständlich befindet sich im Lieferumfang auch eine Lizenz der Backup-Software *IPERIUS*, die ggf. eingesetzt werden kann. Diese ist – idealerweise – jedoch nicht vorinstalliert

Linux-basierendes NAS- und Backup-System

Ausgestattet mit der actidata eigenen NAS- und Backup-Software, die unter anderem neben einer Linux-basierenden Verwaltung der eingebauten Festplatten, dem Volumen-Management, den SMB-Freigaben und dem Zugriffsmanagement auch über ein Backup- und Restore-Tool verfügt. Hierbei können die Daten intern vom Disk-basierenden Speicher auf das eingelegte,

austauschbare DX6-Medium gesichert werden. Die *actidata DX6*-Medien sind somit extern zu lagern und stehen im Bedarfsfall für die Datenwiederherstellung selektiv zur Verfügung.

DX6-Medien speichern die Daten im offenen Format

Die Daten auf den DX6-Medien werden nicht in einem Hersteller-spezifischen Format abgespeichert. Somit folgt actidata auch hier der Strategie des

offenen Standards. Jederzeit ist der Zugriff auch über Fremdsysteme mit handelsüblichen Tools einzusehen bzw. zu extrahieren. Auch auf eine zusätzliche Verschlüsselung der Daten wird verzichtet, denn dieses wird in aller Regel bereits durch die eingesetzte Backup-Software durchgeführt. Zur Verdeutlichung: Das actidata DX6-Medium ist als normale Festplatte über SATA einfach in ein Server-System einzubinden.



Bild: actidata

*actidata DX6 –
Wechselfestplatte als
Backup-Medium.*

Übersicht actidata DX6-Produktfamilie:

Typ	Variante	Betriebssystem	Backup-Software	10GbE-LAN
actidata Qx-DX6	Desktop	actidata Linux	integriert	dual 10GbE
actidata Q-DX6	Desktop	Win Server IoT	offen*	dual 10GbE
actidata RMx-DX6	2U	actidata Linux	integriert	dual 10/25GbE
actidata RM-DX6	2U	Win Server IoT	offen*	dual 10/25GbE
DX6-Medium	3,5 Zoll ext.			

* Windows-basierende Backup-Software in eigener Regie einsetzbar

Konsequent auf 24x7 Server-Komponenten gesetzt

Server-Komponenten, die in der actidata DX6-Produktfamilie eingesetzt werden, sorgen für eine hohe 24x7 Betriebssicherheit und optimale Performance sowohl zu den Produktsystemen über die eingebauten dual 10Gb- bzw. 25Gb-Ethernet-Schnittstellen als auch intern auf die bis zu 900 MByte/h schnellen Festplatte im DX6-Wechselmedium. Server-like verfügen alle Systeme der DX6-Produktfamilie über eine separate IPMI-Board-Management-Schnittstelle.

Service und Support inklusive

Nicht nur alle DX6-Systeme sind mit einer 36monatigen Gewährleistung inklusive eines Vorabaustausch defekter Komponenten ausgestattet, sondern auch die dazugehörigen DX6-Medien. Beides lässt sich optional bis auf 60 Monate servicetechnisch erweitern, so dass hier Investitionen

über einen langen Nutzungszeitraum im Rahmen des *actidata CareFree*-Service abdeckt sind.

Informationen zur DX6-Serie anfordern

Die DX6-Systeme stehen sowohl in der Desktop-, als auch in der 2U-Rackmount-Variante zur Verfügung. Preislich bewegen sich diese je nach Kapazitätsausstattung und Betriebssystem bei einem empfohlenen Verkaufspreis ab 3.100 Euro, netto. Die DX6-Medien liegen beispielsweise mit 8 TByte bei einem Endkundenpreis von 390 Euro, netto. ■

Weitere Informationen:

actidata Storage Systems GmbH

Wulfshofstr. 16 – Indu-Park
44149 Dortmund
Tel. 0231/96 36 32-0
E-Mail: info@actidata.com
www.actidata.com

Bild: via Canva Pro



Karl Fröhlich
speicherguide.de

NIS-2-Richtlinie nimmt Geschäftsleitung in die Pflicht

GESETZLICH VERORDNETE CYBERSICHERHEIT

Cybersicherheit by Design bzw. per Gesetz: Firmen müssen künftig angemessene Sicherheitsmaßnahmen implementieren, um ihre Systeme vor Cyberangriffen zu schützen. So sinnvoll die Anforderungen auch sein mögen, so unausgegoren ist die NIS-2-Richtlinie noch. Wichtig zu verstehen: Die Geschäftsleitung muss selbst Wissen aufbauen.

Die EU verpflichtet Unternehmen per Gesetz zu mehr Cybersicherheit. Die EU-Richtlinie NIS-2 (Network and Information Security Directive 2) muss von den EU-Mitgliedsstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt sein. In Kraft getreten ist NIS-2 bereits am 16. Januar 2023. Einen fertigen Gesetzestext gibt's es allerdings noch nicht. Unternehmen können sich bisher nur

am zweiten Referentenentwurf orientieren, der momentan diskutiert wird.

Der Grundgedanke ist sicher lobenswert: »Das Ziel ist ein besseres gemeinsames Cybersicherheitsniveau«, erklärt **Susanne Moosreiner**, CEO bei **SEP**. »Von NIS-2 sind zirka 30.000 Unternehmen in Deutschland betroffen.«

Die NIS-2-Richtlinie adressiert zunächst Unternehmen mit mindestens 250 Mitarbeitenden oder mehr als 50 Millionen Euro Umsatz und mehr als 43 Mio. EUR Jahresbilanzsumme, die Sektoren mit hoher Kritikalität unterliegen. »Dazu zählen insbesondere die Bereiche Energie, Gesundheitswesen, Verkehr, Banken und Finanzmarktinfrastrukturen, Trink- und Abwasser, digitale Infrastrukturen, Verwaltung von ITK-Diensten sowie Luft- und Raumfahrt«, sagt **Christoph Harburg**, IT-Security Consultant beim Braunschweiger IT-Systemhaus **Netzlink Informationstechnik**. »Diese Unternehmen werden als 'Wesentliche Einrichtungen' bezeichnet.«

Die neue Fassung ersetzt die bisherige Richtlinie NIS-1, die bislang nur für **KRITIS**-Unternehmen (Betreiber von kritischen Infrastrukturen mit wichtiger Bedeutung für das staatliche Gemeinwesen) galt. Betroffen sind nun auch beispielsweise Anbieter digitaler Dienste, Chemie, Ernährung, Medizin, Logistik, Abfallwirtschaft, produzierendes und verarbeitendes



Foto: Netzlink



Christoph Harburg
Netzlink

»Nur wenn klar ist, wo die Lücken sind und wo Verbesserungspotenzial besteht, können geeignete Maßnahmen ausgewählt und ergriffen werden.«

Gewerbe, Forschung und öffentliche Verwaltung (entsprechender Größe).

»Die Branchen sind relativ weit gefasst, aber die Eingrenzung erfolgt über das §28 BSIG (BSI-Gesetz)«, erklärt Rechtsanwalt **Stephan Hansen-Oest** gegenüber *speicherguide.de*. »Dieses besagt, NIS-2 greift für mittlere Unternehmen ab 50 Mitarbeiten-

den oder mehr als zehn Millionen Euro Umsatz bzw. mehr als 43 Mio. Euro Jahresbilanzsumme aus den genannten Sektoren mit hoher Kritikalität.« Das heißt, es ist nicht jede Apotheke oder Arztpraxis automatisch betroffen.

Nur 20 Prozent sind bisher vorbereitet

Richtig vorbereitet sind bisher nur wenige Unternehmen. Nach Einschätzung von **Dennis Weyel**, International Technical Director beim Sicherheitsunternehmen **Horizon3.ai** gehen weite Teile vor allem der mittelständischen Wirtschaft davon aus, von NIS-2 nicht betroffen zu sein: »Das ist ein Irrtum. Unter die Richtlinie fallen nämlich nicht nur die Unternehmen in den vom Gesetzgeber genannten Branchen, sondern auch alle Zulieferer und Dienstleister.«

Eine Stichprobe unter 300 vor allem mittelständischen Unternehmen im Auftrag von Horizon3.ai förderte zutage, dass lediglich 20 Prozent der Firmen bereits Maßnahmen ergriffen haben, um NIS-2 zu genügen. Ein weiteres Viertel gab an, dass ihnen die neuen Sicherheitsanforderungen zumindest »teilweise bekannt« seien und sie entsprechende Maßnahmen planen würden.

Für bemerkenswerte 43 Prozent sind die neuen gesetzlichen Auflagen in Sachen Cybersecurity kein Thema

oder sie sehen keinen Handlungsbedarf. 17 Prozent verlassen sich schlichtweg darauf, dass sich ihre Lieferanten und Geschäftspartner entsprechend auf den aktuellen Stand bringen. Ein knappes Zehntel fühlt sich »ausreichend geschützt«. »Die Ergebnisse lassen auf eine gewisse Blauäugigkeit in Sachen Cybersicherheit



Foto: SEP



Susanne Moosreiner
SEP

»Backup-/ Recovery-Verfahren benötigen künftig eine regelmäßige Integritätsüberprüfung sowie einen Schutz der Backups vor unbefugtem Zugriff.«



Foto: PWS Group



Patrycja Schrenk
PWS Group

»NIS-2 stärkt die Resilienz gegenüber Cyberbedrohungen und gewährleistet eine einheitliche und effektive Sicherheitsstruktur.«

schließen«, analysiert Weyel. Er räumt allerdings ein: »Es wird für viele Mittelständler schlichtweg unmöglich sein, sich rechtzeitig um alle NIS-2-Belange zu kümmern.«

Selbst der **BSI** bezeichnet die personellen, finanziellen und strukturellen Hürden als immens. Die Erhöhung des IT-Sicherheitsniveaus sei zwar alternativlos, noch sei aber nicht sicher, ob Deutschland NIS-2 bis zum Herbst verabschiedet hat. Wichtig sei anzufangen, nicht zuletzt aufgrund des hohen Handlungsdrucks durch die wachsende Bedrohungslage. »Unternehmen sollten anfangen, die Erhöhung ihres Cybersicherheitsniveaus voranzubringen«, rät **Katrin Kubica**, Referatsleiterin beim BSI.

»Der zu erwartende Aufwand wird sicher wegen der umfangreichen organisatorischen Anforderungen hoch und noch ist nicht klar, welche Ausmaße das in Bezug auf die IT und speziell auf das Backup und Recovery hat«, sagt SEP-Chefin Moosreiner. »Besonders die Vorstände und Geschäftsführungen werden in die Verantwortung genommen. Nichtsdestotrotz werden die IT-Manager mit der Umsetzung beauftragt.«

NIS-2-Anforderungen an die Datensicherung

Grundsätzlich sollten alle (betroffenen) Unternehmen eine Backup-Strategie haben und der Aufwand hier

eigentlich überschaubar sein. Trotzdem gilt es zu überprüfen, ob diese passt und an die erhöhten Sicherheitsanforderungen ausreichend angepasst ist, denn es gilt die Geschäftskontinuität sicherzustellen sowie Datenverlust zu verhindern bzw. zu minimieren. »Dazu müssen entsprechende Strategien und auch Techniken verwendet werden, die besten Schutz bieten«, mahnt Moosreiner. »Die bisherige Backup-Strategie ist dahingehend zu überprüfen und bei Bedarf anzupassen. Dazu können Funktionen wie beispielsweise Immutability-Storage und S3 Object-Lock verwendet werden, die eine Unveränderbarkeit der Backup-Daten gewährleisten. Die 3-2-1-1-Regel für Backups (3 Kopien, 2 verschiedene Medien, extern und unveränderbarer Speicher) kann eine weitere Maßnahme sein, bei der die Backup-Daten auf unterschiedliche Speichermedien und Standorte gelegt werden.« Hinzukomme ein gezieltes Monitoring und Reporting über die Backup-Infrastruktur, um die Nachweis-Anforderungen zu erfüllen und Einblicke in die Sicherheit der Backup-Prozesse zu erhalten.

»NIS-2 verlangt, dass Unternehmen kritische Daten und Systeme klar identifizieren und priorisieren«, ergänzt **Deniz Alboyaci**, Director of Sales für die DACH-Region bei **Arcserve**. »Dies bedeutet, dass Backup- und Disaster-Recovery-Strategien so angepasst

NIS-2: Notwendige Maßnahmen

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- grundlegende Verfahren im Bereich der Cyberhygiene (zum Beispiel Updates) und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Quelle: IHK Leipzig

werden müssen, dass diese kritischen Komponenten mit höchster Dringlichkeit und Sicherheit gesichert und wiederhergestellt werden können.«

Auch SaaS-Umgebungen wie *Microsoft 365* müssen IT-Manager mit Nachdruck in die Sicherheitsstrategie einbinden. Backups der Umgebungen seien zwar bereits weit verbreitet, doch wie verhält es sich, wenn nicht

M365, sondern die dahinter liegende *EntraID* angegriffen wird? »Auf solche Fragen müssen Unternehmen zielgerichtet antworten, um NIS-2 Compliant zu sein«, konstatiert Arcserve-Manager Alboyaci.

Die Richtlinie betone zudem die Bedeutung regelmäßiger Tests der Wiederherstellungsverfahren sowie die Simulation von Angriffen, um im

Ernstfall vorbereitet zu sein. Nur durch kontinuierliches Testen sei sichergestellt, dass Backup- und Disaster-Recovery-Strategien tatsächlich funktionieren. »NIS-2 bringt also nicht nur formelle Änderungen, sondern fordert Unternehmen auf, ihre Backup- und Disaster-Recovery-Strategien grundlegend zu überdenken und zu erweitern«, sagt Alboyaci. »Firmen, die

diese Anforderungen vernachlässigen, riskieren nicht nur die Nichterfüllung gesetzlicher Vorgaben und öffnen das Tor der persönlichen Haftbarkeit, sondern setzen ihr eigenes Unternehmen und deren Mitarbeiter aufs Spiel.«

Sollte ein Sicherheitsvorfall eintreten, ist ein effektives Krisenmanagement entscheidend, um schnell, fristgerecht und mit angemessener Reaktion zu handeln. »Unternehmen sollten hier klare Verfahren und Protokolle für die Erkennung, Bewertung

und Bewältigung von Sicherheitsvorfällen entwickeln und auch an ein effektives Backup-Management sowie Wiederherstellungsverfahren denken«, rät **Patrycja Schrenk**, Geschäftsführerin der **PSW GROUP**. »Unternehmen, die die Anforderungen der NIS-2-Richtlinie nicht erfüllen, riskieren erhebliche Geldbußen von bis zu zehn Millionen Euro oder zwei Prozent des Jahresumsatzes. Zudem können leitende Organe persönlich haftbar gemacht werden.«

Jetzt auf das Cybersicherheitsgesetz vorbereiten

Für alle, die noch nicht wirklich aktiv geworden sind, heißt es nun, Anfangen! Das heißt prüfen, ob man in den Anwendungsbereich der NIS-2-Richtlinie fällt und sich dann beim *Bundesamt für Sicherheit in der Informationstechnik* (BSI) registrieren. »Anschließend ist eine gründliche Risikoanalyse unerlässlich, um potenzielle Schwachstellen und Risiken in den eigenen Netz- und Informationssys-

temen zu identifizieren«, meint Schrenk.

Basierend auf den Ergebnissen dieser Analyse sollten angemessene technische und organisatorische Maßnahmen implementiert werden, um diese Risiken zu minimieren und die Sicherheit der Systeme – einschließlich der Lieferkette – zu verbessern. »Der Einsatz von Kryptografie und gegebenenfalls Verschlüsselungstechnologien ist in diesem Zusammenhang eine Maßnahme, um sensible Daten zu schützen«, erklärt Schrenk. »Darüber hinaus empfehlen sich auch Maßnahmen zur Personalsicherheit, Zugriffskontrolle und Asset Management, um unbefugten Zugriff zu verhindern. Eine Multi-Faktor-Authentifizierung oder eine kontinuierliche Authentifizierung tragen übrigens dazu bei, die Sicherheit von Zugriffen zu erhöhen.«

Kommunikationskanäle für Sprach-, Video- und Textkommunikation sollten so ausgelegt sein, dass sie auch während eines Sicherheitsvorfalls eine unterbrechungsfreie Kommunikation gewährleisten. Zudem sollten Beschäftigte gemäß NIS2-Richtlinie jetzt regelmäßig in Cybersecurity geschult werden, um sie für Sicherheitsrisiken zu sensibilisieren. Auch ein effektives Krisenmanagement ist entscheidend, um bei einem Sicherheitsvorfall schnell, fristgerecht und mit angemessener Re-

aktion zu handeln. Unternehmen sollten hier klare Verfahren und Protokolle für die Erkennung, Bewertung und Bewältigung von Sicherheitsvorfällen entwickeln und auch an ein effektives Backup-Management sowie Wiederherstellungsverfahren denken.

»Um bei den NIS-2-Anforderungen den Überblick zu behalten, ist ein schrittweises, strukturiertes Vorgehen der effizienteste Weg für Unternehmen«, empfiehlt Netzlink-Manager Harburg. »Der Kern ist dabei die Gegenüberstellung der IST-Situation eines Unternehmens in Sachen IT-Sicherheit mit der SOLL-Situation. Nur wenn klar ist, wo die Lücken sind und wo Verbesserungspotenzial besteht, können geeignete Maßnahmen ausgewählt und ergriffen werden.«

Die Geschäftsführung sollte sich zunächst eingehend mit ihren Pflichten und möglichen Sanktionen auseinandersetzen und sich schulen lassen. Mit diesem Wissen ausgestattet, kann sie dann entscheiden, welche Maßnahmen zur Umsetzung der Anforderungen notwendig sind und wie die Verantwortlichkeiten und Prozesse innerhalb des Unternehmens verteilt werden. ■

Anmerkung der Redaktion

Die Cybersicherheit zu erhöhen ist für Unternehmen systemrelevant und absolut zu begrüßen. Es gibt unzählige Beispiele für erfolgreiche Cyberangriffe. Wer hier noch trödelt und sich nicht angesprochen fühlt, dem ist vermutlich eh nicht zu helfen. Richtlinien wie NIS-2 sind sinnvoll, um eine einheitliche Basis zu schaffen. Im Prinzip sind die Fachmedien und die Postfächer gerade voll mit Geschreibsel zu NIS-2. Wie Sie gerade lesen, sind wir auch dabei.

Nun gibt es genug Stimmen, die behaupten, es fühlen sich noch zu wenige angesprochen. Das hat aus meiner Sicht einen ganz klaren Grund: Die Bezeichnung NIS-2 ist nicht selbsterklärend. Wir haben alle genug Themen auf dem Tisch, da rufe ich doch keinen Themenschwerpunkt »NIS-2« auf, klicke keine entsprechenden Banner an oder interessiere mich für ein eBook dazu.

Die verantwortlichen Stellen müssen so etwas viel besser vorbereiten und erklären. Mich stört auch, dass im Herbst ein Gesetz umgesetzt werden soll, das jetzt rund drei, vier Monate vorher noch nicht fertig ist. Da wird wieder vieles mit der heißen Nadel gestrickt und mit dem Einblick, den ich bisher habe, befürchte ich

ein überhöhtes Maß an Bürokratie (Dokumentationspflicht).

Gut ist, dass die Überwachungspflicht direkt der Geschäftsleitung obliegt. Diese kann hier nicht mehr das Wissen delegieren, sondern muss sich selbst darum kümmern. Die Verantwortlichen müssen sich des Risikos bewusst sein, wenn sie an der IT-Sicherheit sparen. Wobei das in der Praxis vermutlich anders gelebt wird. Letztendlich bleibt ja doch alles an der IT-Abteilung hängen, inklusive der internen Verantwortung.

Und Achtung: Grundsätzlich sollte jedes Unternehmen NIS-2 erfüllen, um sich bestmöglich vor Cyberangriffen zu schützen. Nur halt ohne dem gesetzlichen Druck und Nachweisgedöns. Außerdem ist davon auszugehen, dass betroffene Firmen per Compliance-Vorschriften nur noch mit Partnern und Lieferanten zusammenarbeiten wollen, die eine angemessene Cybersicherheit pflegen.

Karl Fröhlich, *speicherguide.de*



Weitere Informationen:

NIS-2: Informationen des BSI



Michael Baumann
speicherguide.de

Anforderungen an IT-Infrastruktur durchaus komplex

STORAGE FÜR KI IM MITTELSTAND

Künstliche Intelligenz ist inzwischen ein wichtiger Bestandteil der digitalen Transformation. Die Datenverarbeitung auf KI-Basis soll Optimierungen und Innovationen ermöglichen, verlangt aber auch eine anspruchsvolle Storage-Infrastruktur. Für KMU und Mittelstand eine besondere Herausforderung.

Laut diverser Studien (EY 2023, Deloitte 2024) haben über 50 Prozent deutscher Großunternehmen 2023 in KI investiert – mit steigender Tendenz. Allerdings kommt der **Bitkom** Ende 2023 zu dem Ergebnis, dass bei deutschen Firmen ab 20 Mitarbeitern nur 15 Prozent künstliche Intelligenz (bewusst) einsetzen. 70 Prozent verstehen KI als Chance. Im internationalen Vergleich hinkt sie zeitlich etwas hinterher, allerdings geben die Zahlen das ab und an verkündete »Abgehängtsein« der deutschen Wirtschaft nicht her.

Hindernisse und Chancen

Beklagt werden weniger Sicherheitsbedenken, vielmehr Fachkräftemangel und fehlende gesetzliche Rahmenbedingungen. Und natürlich die deutsche Dateninfrastruktur. Ohne schnelle Netze kaum eine KI.

Aus Speichersicht ist aber für manche KMU auch einfach das Problem, dass die viel zitierte riesige Menge an relevanten Daten für gewinnbringende KI-Analysen, Machine-Learning, Deep-Learning und Large-Language-Models aus dem eigenen Unternehmen zunächst fehlt. Dann kann ein kompletter Übertrag in die Cloud der einzig gangbare Einstieg in die KI-Welt sein. Für andere gilt: Eine Voraussetzung für den Einsatz von KI ist die richtige Ausstattung mit Technologie.

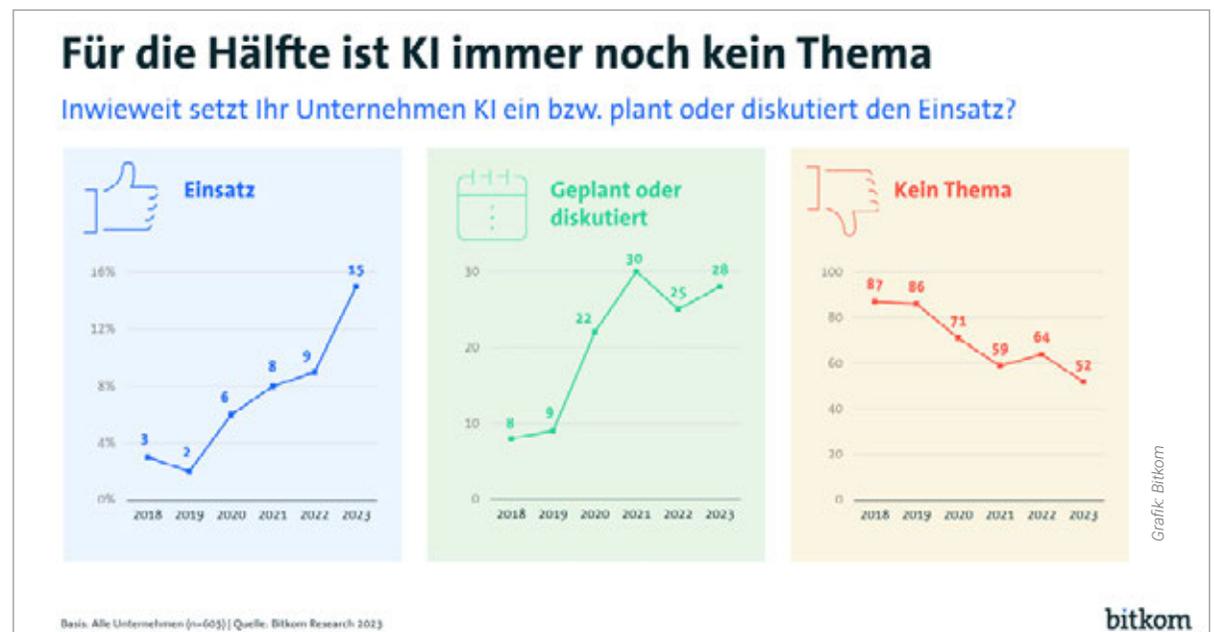
Einsatzbereiche findet der Mittelstand laut der Studie »Künstliche In-

telligenz im Mittelstand« der **WiK Consult** im Auftrag des **Bundesministeriums für Wirtschaft und Klimaschutz** (Dez. 2023) zur Genüge: Automatisierung in Produktion, Kundenservice, Logistik und Lieferkettenmanagement, Vertrieb mit automatisierter Priorisierung, individualisiertes Marketing, Entwicklung oder Finanzmanagement. Ziele sind unter anderem Kosteneinsparung, erhöhte Effizienz und die Optimierung bestehender Prozesse und die Entwicklung neuer Geschäftsfelder durch innerbetriebliche Innovation.

Was ist die richtige Ausstattung mit Technologie?

Einfache Antwort: KI benötigt neue Compute-Kapazitäten, schnelle Datenübertragung in und zwischen Systemen und Plattformen, schnellen Speicher und die Möglichkeit, große Datensätze für die Analyse vorzuhalten. Also alles High-Performance? Nicht nur: Schließlich müssen die Daten auch gesichert, für Disaster-Recovery-Aufgaben und Archivierung für etwaige Compliance-Anforderungen vorgehalten werden.

Das macht die KI für KMU und Mittelstand mitunter recht komplex. Zwar hat jeder namhafte Anbieter KI-optimierte Storages im Angebot. In den wenigsten Fällen dürfte eine Appliance allein die erhofften, adäquaten Ergebnisse liefern.



Einsatz von KI in deutschen Unternehmen 2023

Viele KI-Anwendungen arbeiten mit einer Kombination aus lokaler Infrastruktur, Cloud-Ressourcen und hybriden oder Multi-Cloud-Architekturen. Gerade für KMU ein Bereich, der mit externer Expertise vor Fehlinvestitionen und enttäuschten Erwartungen geschützt werden sollte. Und damit beginnt im ersten Schritt die Evaluation, sprich eine Datenklassifizierung oder auch die Identifizierung von Workload-Mustern, sowie die Definition von Zielen sind Voraussetzung. Ein Chatbot benötigt weniger Ressourcen als eine Deep-Learning-Anforderung.

Anforderungen an KI-Speicherarchitekturen

1. Performance

Geringe Latenz und hohe I/O-Leistung sind Trumpf. Auf dem Wunschzettel steht eine parallel arbeitende, hochperformante I/O-Speichersystem-Architektur, die über Fabrics mit NVMe (NVMe-oF) kommuniziert und NAND-Flash (TLC oder günstiger QLC) und *Storage Class Memory* integriert, wobei Blöcke, Files und Container in einer Scale-out-Architektur verwaltet werden. Auf den Platinen arbeiten neben den CPU neuester Generation ausrei-

chend GPUs, auch *Compute Express Link* (CXL) darf unterstützt werden.

Wer Wünsche und Kosten abgleicht, und das tut der Mittelstand in der Regel, wird je nach Anforderung entsprechende Abstriche machen und dennoch Ziele erreichen können.

2. Skalierbarkeit

KI-Daten wachsen rasant. Hier muss der passende Mix gefunden werden für eine skalierbare Infrastruktur aus lokalen (SAN-)Systemen, Objektspeichern und eventuell Scale-out-Dateisystemen. Reine SAN-Systemlösun-

gen dürften in Sachen Skalierbarkeit und Kosten weniger tauglich sein, die Cloud birgt Performance-Einschränkungen.

3. Verfügbarkeit und Beständigkeit

KI-Berechnungen können Tage oder Wochen dauern. Entsprechend werden Ressourcen beansprucht. Einzelne Komponenten sollten im Idealfall einfach austauschbar sein. Die Verfügbarkeit von Daten wird durch Storage-typische Sicherungsmechanismen für Ausfallsicherheit, Backup und

Disaster-Recovery oder Erasure-Coding gewährleistet. Auch darf nicht außer Acht gelassen werden, dass eine KI-Infrastruktur ständigen Optimierungsbedarf mit sich bringt. Das beinhaltet auch Komponenten und deren Aktualisierung.

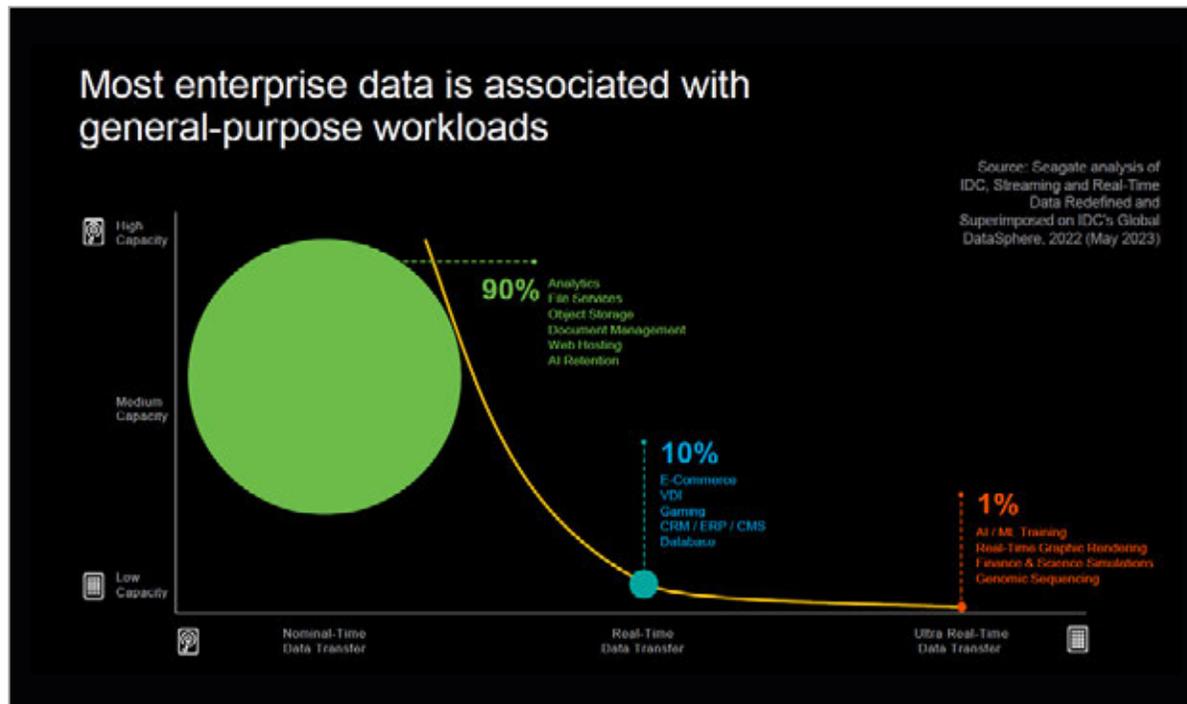
4. Integration

Eine desaggregierte Speichernetzwerkplattform muss sich möglichst nahtlos in die Compute-Umgebung und in das Netzwerk mit hoher Bandbreite integrieren und auch mit einzelnen Systemupdates funktionieren.

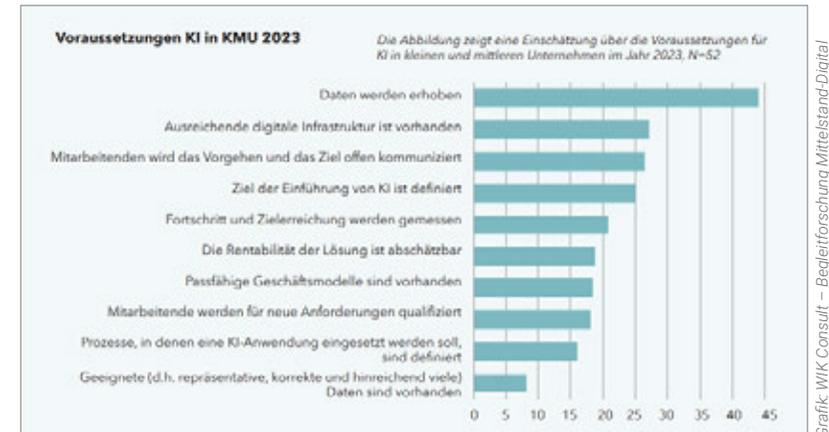
Allerdings: Egal wie sorgfältig man plant, einen Flaschenhals wird das Gesamtsystem behalten.

5. Preis: High-Performance und HDD?

KMU und Mittelstand versprechen sich wohl zurecht Optimierungen, Kosteneinsparungen und Innovationschancen, auch für neues Geschäft. Dennoch hängt das Ausmaß der KI-Einstiegs massiv vom Preis ab. Studien zum Return on Investment und Systemgesamtkosten sind uns nicht bekannt.



Nur ein Bruchteil der Unternehmenspeicher muss Echtzeit-Daten verarbeiten.



Voraussetzungen für den KI-Einsatz bei KMU

Grafik: WIK Consult – Begleitforschung Mittelstand-Digital

KI: Hybride Speicher die Zukunft

»Letztlich steht NVMe für Kosteneinsparung und Investitionssicherheit, auch und gerade für KMU und Mittelstand«, sagt beispielsweise **Sven Meyerhofer**, Geschäftsführer bei der **N-TEC**, auch mit Blick auf KI. »Für mittelständische Unternehmen sind NVMe-SANs eine lohnende Investition, um die IT-Infrastruktur zu modernisieren und die Leistungsfähigkeit zu steigern. Dies ermöglicht es mittelständischen Unternehmen, wettbewerbsfähig zu bleiben und auf zukünftige Herausforderungen vorbereitet zu sein.«

Einen anderen Standpunkt zum Thema vertritt **Hugo Bergmann**, Senior Product Marketing Manager bei **Seagate**: »Laut mehrerer Analysten ist Flash nach wie vor sechsmal so teuer wie die HDD, und das wird sich absehbar nicht ändern. Deswegen behält die Festplatte auch im KI-Um-

feld ihre Berechtigung.« Die Weiterentwicklung an Speicherdichte und Kapazitäten laufe Kopf an Kopf weiter, nur dass der Gesamtbedarf allein durch Flash gar nicht gedeckt werden könne. Das sei aber auch nicht notwendig, da nur etwa zehn Prozent der aktiven Online-KI-Operationen den hoch performanten NAND-Flash oder auch GPU-Unterstützung benötigen würden.

»Nachgelagert braucht auch KI mit LL-Modellen und Gen AI ein Datenarchiv«, meint Bergmann. »Schon aus Compliance-Gründen muss KI abgesichert werden. Wer es sich leisten möchte, kann dafür Flash nutzen, aber für diese Zwecke ist die moderne HDD absolut ausreichend und eben deutlich kosteneffizienter. Für uns ist eine hybride Architektur aus lokaler Festplatte und Flash auch im KI-Umfeld die Zukunft.«

Sicheres Backup als Schutz vor den Folgen von Ransomware Attacken

Ein Angriff durch Ransomware ist für ein Unternehmen immer eine Katastrophe. Allein das Schützen des Netzwerk vor weiteren Angriffen erfordert oft viele Tage. Ist dann auch noch das Backup der Unternehmensdaten von der Attacke betroffen, kann das den Ruin bedeuten.

Den besten Schutz des Backups bieten natürlich nach wie vor **ausgelagerte LTO-Kassetten**, da hier jede Art von Remote-Zugriff zu 100% ausgeschlossen werden kann. Auch bei Libraries sollten die Kanister mit dem Backup am besten entnommen werden.

Doch auch die Hersteller von **diskbasiertem Backup** haben einiges getan, den Zugriff auf die Datensicherungen zu verhindern. Minimum der Anforderungen ist, dass die Daten nur für die Backupsoftware selbst sichtbar sind. Das ist z.B. bei **Open-E JovianDSS** der Fall, wenn die Daten snapshotbasiert auf einen weiteren Rechner gesichert werden.



EonStor GS 1000 Gen2

Ebenso macht es mittlerweile auch **Infotrend** mit ihren **EonStor GS** Systemen. Hier kommt eine **Data-Lock** Funktion dazu, die Backup-Volumes unveränderlich macht.

Außerdem bietet Infotrend die

Möglichkeit, selbständig Backups zu ziehen, sowie **S3 Immutable Backupvolumes für Veeam** zur Verfügung zu stellen.

Sehr elegant hat das **ExaGrid** gelöst: Hier werden die Backups nach Auslagerung in eine **zweite Repository-Ebene** (mit Deduplikation

auch über viele Knoten) gesichert. Dort können sie mit einer einstellbaren **Retention Time** vor jeder Veränderung geschützt werden. Bei **Veeam**, der idealen Software für die Sicherung virtueller Maschinen, lässt sich ein Linux Server zum **Hardened Linux Immutable Repository** machen, das nur von der Software direkt erreicht werden kann und ebenso durch Retention Zeiten geschützt wird.

Backuplösungen mit Schutz vor Ransomware bei EUROstor:

(mehr Info unter www.EUROstor.com/backup.)

- **LTO Tape Libraries von Actidata**
Schutz der Daten durch räumliche Auslagerung 
- **Veeam Backup Server**
Zweit-Sicherung der Virtuellen Maschinen in ein Immutable Repository (s. rechts) 
- **ExaGrid Tiered Backup Storage**
Backups mit Retention in einer zweiten Backupenebene 
- **Infotrend EonStor GS**
Volumecopy mit Schreibschutz durch Data-Lock Funktion und als S3 Speicher für Veeam Repository 
- **Open-E JovianDSS Storage**
snapshot basierte On-/Off-site Data Protection (ODP) auf zweiten Standort 



Alle Storage-Systeme aus einer Hand:

EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, Scale-Out Clustern und Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die

Virtualisierung. Dazu kommen RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches.

Rufen Sie uns einfach an, wir beraten Sie gerne! Registrieren Sie sich auch für unseren Storage Newsletter (Print oder E-Mail, 3 x pro Jahr) unter www.EUROstor.com/Newsletter.



VEEAM AMD EPYC



ES-3036 als Hardened Linux Immutable Repository mit 36 Slots (12 davon auf der Rückseite)

ES-3036, 36 3.5" Slots, z.B. teilbestückt mit **inkl. MwSt. € 13.078,10** **exkl. MwSt. € 10.990,-**
12 x 20 TB SATA Enterprise HDDs,
2 x 512 GB M.2 Boot-SSD für das Betriebssystem

Hardened Linux Backup Repository Server:

- Storage-Server mit 36 3.5" Slots, bis 864 TB bei Verwendung von 24 TB Disks
- alternativ: 12/16/24 3.5" Slots, 24/72 2.5" Slots
- AMD EPYC Rome 7232P Prozessor, 8 Core, 3,1 GHz auf Supermicro H12SSL-NT Board, 7 PCIe 4.0 Slots
- 64 GB RAM, optional bis zu 1 TB
- 2 x 10 GbE (RJ45) onboard, opt. mehr und bis 100 GbE
- OS auf 512 GB NVMe M.2 SSDs im RAID 1, Ubuntu auf Wunsch vorinstalliert
- Areca RAID Controller mit 12 Gbit SAS, RAID Management über dedizierten Netzwerkport
- optional Erweiterungsports für bis zu 512 Laufwerke
- Monitoring, remote Management und iKVM Console über Netzwerk (IPMI)
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt • Tel: +49 (0)711 70 70 91 70 • Fax: +49 (0)711 70 70 91 60

Preisänderung, Druckfehler und Irrtum vorbehalten.

Informieren und registrieren Sie sich auf unserer Website: www.EUROstor.com/Newsletter

E-Mail: Info@EUROstor.com - Tel.: +49 (0)711 70 70 91 70

Bild: ChatGPT/DALL-E



Karl Fröhlich
speicherguide.de



Jens Leischner
speicherguide.de

Unwort der IT-Branche 2024: Vmware

VMWARE AKTUELL (NOCH) UNUMGÄNGLICH

Die Unzufriedenheit mit Vmware wächst: Preiserhöhungen und eine umstrittene Strategie des neuen Eigentümers Broadcom lösen Unmut aus. Trotz des Entwicklungsvorsprungs und der Herausforderungen, die eine Migration mitsichtbringt, ist der Ruf nach Alternativen laut. Noch decken diese allerdings nicht alle Bedürfnisse ab.

Virtualisierung und eine mögliche Abkehr von **VMware** ist aktuell Branchen-Thema Nummer 1. Alle sind geschockt bezüglich der Preisentwicklung und des Geschäftsgebarens des neuen VMware-Besitzers. Auf der *Storage Technology-Konferenz des DLR* wurde »VMware« sogar zum IT-Unwort des Jahres ernannt. Zwar prüft derzeit nahezu jede IT-Abteilung mögliche Alternativen, allerdings so richtig ran traut sich keiner. Noch.

VMware zu migrieren, ist im großen Stil ein aufwändiges Projekt. Auch sich auf einen neuen Vertragspartner einzulassen, hält viele noch zurück. Größere Unternehmen sind zudem noch an Rahmenverträge gebunden, aus denen man sich erstmal lösen musste.

Fakt ist allerdings – bei allem Unmut – VMware hat einen enormen Entwicklungsvorsprung. Im Enterprise-Bereich kann momentan keine der Alternativen VMware ersetzen. Partiiell gesehen natürlich schon, aber nicht in seiner Gesamtheit. Und dies weiß man auch bei **Broadcom**.

VMware: Enormer Wertzuwachs

Während sich die Branche letztes Jahr noch fragte, warum ein Netzwerkhersteller eine Virtualisierungs-Software kauft, witterte man dort eventuell schon das große Geschäft. Immerhin war die Investitionssumme immens und der Wertzuwachs von VMware ebenfalls. Zur Erinnerung:

- 2003 kauft EMC VMware für 635 Millionen US-Dollar
 - 2015 kauft **Dell** für 67 Milliarden US-Dollar EMC, inklusive VMware
 - 2023 kauft Broadcom für zirka 70 Milliarden US-Dollar VMware von Dell
- VMware war mehr als nur Client-OS-Virtualisierung, sondern mit NSX, vSAN, Load-Balancer, Firewall und weiteren Produkten auch im Netzwerkumfeld vertreten und in den Produkten von Dell EMC gut integriert. Aus diesem Grund dachte jeder, dass das passt und wird weiterentwickelt. Was aber Anfang des Jahres passierte, schockte die Kunden.

Produkte wurden abgekündigt wie zum Beispiel *vSphere Remote Office* und ein gänzlich neues Lizenzmodell (Abo-Modell inklusive Kapazitätsabhängigkeit) eingeführt. Zudem wurden Produkt-Bundles erstellt. Laut VMware geschah dies natürlich alles im »Sinne« des Kunden. Diese sind angesichts von Preiserhöhungen von bis zu über 100 Prozent eher fassungslos. Es verwundert daher nicht, dass sich alle auf die Suche nach Alternativen begeben.

Hier bieten sich zunächst **Microsoft** mit *Hyper-V* sowie **Citrix XenServer**, *KVM*, *Proxmox* und *XCP-ng* an. Alle haben ihre Vor- und Nachteile. Das Entscheidende ist aber, eine Migration von VMware auf ein anderes Produkt ist meist nicht so schnell, geschweige einfach möglich.

Das weiß auch Broadcom-CEO **Hock Tan**. Irgendwie müssen die 70 Milliarden ja wieder reinkommen. In diesem Fall, und darin sind sich Kunden und Experten einig, wurde die Marktmacht von VMware schamlos ausgenutzt, um den höchstmöglichen Profit zu erwirtschaften. Rücksichtslos hat der Hersteller damit auch das Vertrauen zu seiner Kundenbasis zerstört. Es verwundert nicht, dass dieses Vorgehen die EU-Kartellbehörde auf den Plan gerufen hat. VMware sieht dies natürlich gänzlich anders.

VMware trennt sich vom Endnutzer-Computing

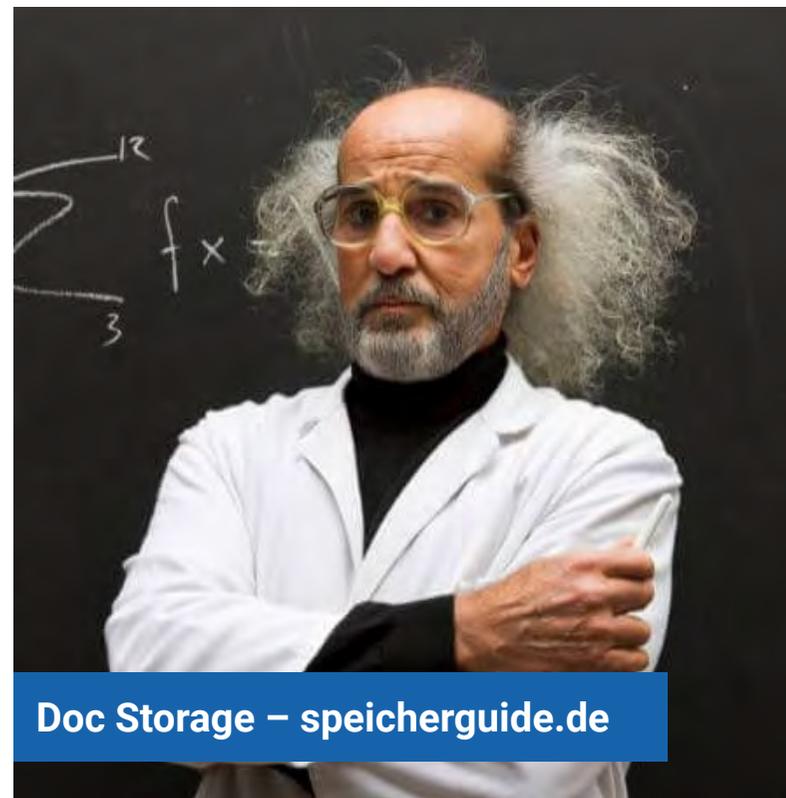
Während der Finanzmitteilung des Unternehmens für das vierte Quartal 2023 bestätigte CEO Tan offiziell, dass Broadcom beabsichtigt, sich vom Endbenutzer-Computing zu trennen. Somit werden in Zukunft keine virtuellen Desktop-Infrastrukturlösungen wie *VMware Horizon* mehr angeboten. Im Februar dieses Jahres gab das Investmenthaus *KKR* bekannt, eine endgültige Vereinbarung zur Übernahme der EUC-Abteilung von Broadcom getroffen zu haben. Durch diesen Abschluss wird die EUC-Abteilung (End User Computing) zu einem eigenständigen Unternehmen.

Im Rahmen der Abkehr von der unbefristeten Lizenzierung wurde die freie Lizenz *VMware vSphere Hypervisor* (Free Edition) laut Broadcom

EOGA (Ende der allgemeinen Verfügbarkeit) gesetzt. Derzeit ist kein gleichwertiges Ersatzprodukt verfügbar oder in Planung.

Broadcom setzt auf Abonnement-Zwang

Durch die Übernahme von VMware treibt Broadcom den Zwang auf Abon-



»Es stellt sich die Frage, will man das weiter unterstützen. Zunächst sollte man in den sehr sauren Apfel beißen und bei VMware bleiben, wenn es den eigenen Anforderungen entspricht.«

➔ **VMware: Wahnsinn nicht weiter unterstützen**

nement-Software für alle VMware-Produkte voran. Um Kunden zum Abschluss eines Software-Jahresabonnements zu bewegen, hat man den Preis der VMware Cloud Foundation gesenkt. VMware Cloud Foundation ist Broadcoms neues Flaggschiff-Hybrid-Cloud-Angebot der Unternehmensklasse, mit dem Kunden ihre geschäftskritischen Anwendungen belastbar und kosteneffizient ausführen sollen. Momentan noch gibt es einen Rabatt, allerdings ist nicht absehbar, wie lange noch.

Damit hat Broadcom eindeutig den Weg von Adobe eingeschlagen und betrachtet die Bereitstellung von Software ausschließlich als Cloud-basierter Dienst. In Kombination mit der Schließung bestehender Vertriebskanäle für VMware-Partner und der Einstellung ihrer On-Prem-Software muss sich das gesamte Software-Asset-Management auf vollkommen neue Einkaufszwänge einstellen. Viele Anwender werden gleich den Entwurf einer vollkommen neuen Architektur in Betracht ziehen, da in den meisten Umgebungen die Verwendung nicht unterstützter Software untersagt ist.

Massiver Stellenabbau bei VMware erwartet

Es wird, trotz all dem hochtrabenden Manager-Analysten-Sprech in Konferenzen und Interviews, zu einem mas-

siven Stellenabbau bei VMware kommen. Das Unternehmen versucht, den größtmöglichen Mehrwert aus den 69 Milliarden US-Dollar herauszuholen, die man für die VMware-Übernahme ausgegeben hat. Die Änderungen bei der Software-Lizenzierung bedeuten auch, dass die meisten Kunden nicht mehr mit ihrem gewohnten VMware-Partner zusammenarbeiten werden.

Ein Analysten-Blog meinte hierzu: »Natürlich wurden Einsparungen erwartet – Broadcom hatte zuvor festgelegt, dass man nach Abschluss des Deals 250 Millionen US-Dollar an `Synergien` finden könne, und VMware-Mitarbeiter wurden bereits Anfang des Jahres davor gewarnt.« Dann kam es zu den ersten Entlassungen. Weiterhin wies der Analyst darauf hin, dass Broadcom die Rückkehr zum Büroarbeitsplatz vorschreibt und damit die Hybridvereinbarungen von VMware aufkündigt. Auch das wird für viele Mitarbeiter eine sehr unpopuläre Entscheidung sein. Mit Blick auf bestehende VMware-Partner wurde festgestellt: »Für die zum Teil langfristig gebundenen Partner besteht das Problem darin, dass dies alles mit vollkommen neuen Vertragsbedingungen und der ständigen Angst vor möglichen Preiserhöhungen einhergeht. Broadcom hat bereits angekündigt, dass es einen schnellen Übergang von unbefristeten Lizenzen zu laufenden Abonnements wünscht.« Abonnements kosten mit der Zeit al-

lerdings selten weniger als klassische Käufe und erfordern von den Kunden ganz andere Bestell-, Buchungs- und Abrechnungsverfahren.

Noch ist VMware relativ safe

Bisher wurde VMware durch die Position als etablierter Anbieter und Kreativeur eines neuen Segmentes einigermaßen geschützt. Viele IT-Verantwortliche testen momentan vor allem Alternativen aus dem Open-Source-Umfeld. Sie müssen allerdings feststellen, dass ein Großteil der in den Unternehmen laufenden Software nur als vSphere-basierte virtuelle Appliances verfügbar sind. Daher sollte man – zunächst – in den sehr sauren Apfel beißen und bei VMware bleiben, wenn es den eigenen Anforderungen entspricht.

Gleichzeitig wird ein Plan B entwickelt. Wer weiß, auf welche Ideen – vor allem im Bereich der Preisliste – Broadcom in Zukunft noch kommt, um sich die 69 Milliarden mit etwas Ertrag zurückzuholen. Wie wir hören, arbeiten viele an sogenannten Leuchtturmprojekten als Alternative zu VMware. Einerseits um einen Wechsel zu ermöglichen, andererseits um Broadcom zu stellen: »Wir haben eine Alternative, ändert Euer Geschäftsmodell.«

Für den Erhalt der bisherigen Infrastruktur spricht auch das in die zuständige Mannschaft investierte Training. Die hierbei speziell für VMware

erworbenen Kenntnisse wären bei einem Wechsel annähernd wertlos. Wobei eine gewonnene Erfahrung in der IT immer etwas Wert ist und ein Hersteller-, Produkt- und Strategiewechsel auch nicht gänzlich unüblich ist.

Cloud als VMware-Ersatz

Eine ebenfalls diskutierte Möglichkeit ist, die lokale auf VMware betriebene Umgebung vollständig in eine extern betriebene Cloud zu verschieben. Damit entbindet man sich von einem bestimmten Hersteller, so ein Argument der Befürworter. Kritiker bemängeln, dass man sich damit in Abhängigkeit eines Cloud-Providers begibt.

Preiswerter wird es meist nicht, denn oft genug explodieren die Kosten mittelfristig regelrecht. Während in einer Netzwerkumgebung die Rechtevergabe sehr stark reglementiert ist, kann in der Cloud quasi jeder kaufen was und so viel er will. Hier wird eine starke und einschränkende Verwaltung benötigt, die es aber selbst aufzusetzen gilt und nicht einfach als Cloud-Baustein hinzugebucht werden kann.

Für größere Umgebungen fehlt es momentan an einem brauchbaren VMware-Ersatz. Hyper-V ist noch am weitesten, kann aber nicht alles abdecken. Knackpunkte sind insgesamt unter anderem das Datastore-Management, das automatische Ver-



schieben von Daten sowie das Einbinden von Monitoring und Datenbanken. Auch das Backup ist bei den verschiedenen Alternativen noch nicht allumfassend gelöst. Aktuell heißt es abwarten, wie schnell die Alternativanbieter ihre Hausaufgaben abgearbeitet bekommen. ■

Newsletter-Abonnenten erhalten die neue Ausgabe jeweils »linkfrisch« an ihren Mail-Account. Registrieren Sie sich **bitte hier**. Beachten Sie auch unser Archiv im **Download-Bereich**.

**storage-magazin.de**

eine Publikation von speicherguide.de
Karl Fröhlich
Ginsterweg 12, 81377 München
Tel. +49 (0) 89-740 03 99
E-Mail: redaktion@speicherguide.de

Chefredaktion, Konzept:

Karl Fröhlich (*verantwortlich für den redaktionellen Inhalt*)
Tel. 089-740 03 99
E-Mail: redaktion@speicherguide.de

Redaktion:

Michael Baumann, Karl Fröhlich, Jens Leischner, Peter Marwan

Schlussredaktion:

Michael Baumann, Brigitte Scholz

Titelbild:

ChatGPT/Dall-E

Layout/Grafik:

Uwe Klenner, Layout und Gestaltung,
Rittsteiger Str. 104, 94036 Passau,
Tel. 08 51-9 86 24 15
www.layout-und-gestaltung.de

Mediaberatung:

Bettina Röber
Tel. +49 177 8487001
E-Mail: broeber@speicherguide.de

Urheberrecht:

Alle in »storage-magazin.de« erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte (Übersetzung, Zweitverwertung) vorbehalten. Reproduktion, gleich welcher Art, sowie elektronische Auswertungen nur mit schriftlicher Genehmigung der Redaktion. Aus der Veröffentlichung kann nicht geschlossen werden, dass die verwendeten Bezeichnungen frei von gewerblichen Schutzrechten sind.

Haftung:

Für den Fall, dass in »storage-magazin.de« unzutreffende Informationen oder Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit der Redaktion oder ihrer Mitarbeiter in Betracht.

Unser Team



” **Karl Fröhlich**
Chefredakteur
speicherguide.de



” **Michael Baumann**
Redaktion
speicherguide.de



” **Peter Marwan**
Redaktion
speicherguide.de



” **Jens Leischner**
Redaktion
speicherguide.de



” **Bettina Röber**
Mediaberatung
speicherguide.de