

■ STRATEGIE

Storage- & IT-Beschaffung
wird schwieriger

■ SOUVERÄNITÄT

Eigentum, Kontrolle und
US-Rechtsrisiken

■ SICHERHEIT

Zero-Trust: KI verändert
die Spielregeln

Sicher Planen in
Unsicheren Zeiten

36 Seiten
geballtes
Storage-Wissen

Einkaufsführer Storage 2026



Doc Storage.

Jetzt auch auf **YouTube**.

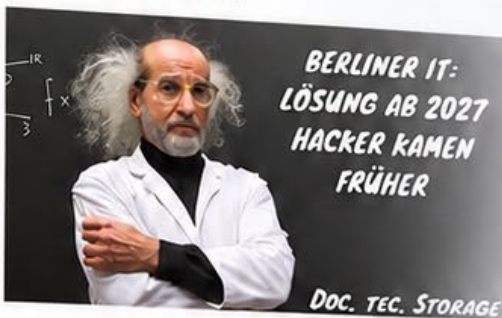
speicherguide.de
Das Storage-Magazin

News Storage Backup Datacenter Infrastrukturen Management Security

Kennen Sie bereits unseren Newsletter? ☐

18.09.2026

Berlin – das EDV-Shithole...



Berlin wusste seit Jahren, dass sein Landesnetz für Verschlusssachen nicht ausreichend gerüstet war. Trotzdem blieb es bei Zwischenlösungen, Einzelrechnern und Papierakten. Dann kamen die Angreifer früher als die geplante Lösung. Doc Storage kommentiert behörden-IT zwischen Versäumnissen, Aktionismus und erstaunlicher Gelassenheit.

Kommentar Doc Storage:

Ernsthaft!!! Nach langer Zeit muss ich mal wieder. Man hält es ja nicht mehr aus!

Berlin. In einer auf den 2. Dezember 2024 datierten internen Unterlage, die laut Medienberichten für die Senatssitzung am 25. Februar 2026 bestimmt war, benennt die Innenverwaltung eine bislang bestehende Fähigkeitslücke: flächendeckende Lagerung, Empfang und Versand von Verschlusssachen. Unterlagen der Stufe VS-NID können nicht über den normalen Dienstweg verteilt werden. Nur per Hauspost oder verschlüsselt.

Im April 2025 hält eine Handreichung der Senatskanzlei fest: »Das Berliner Landesnetz ist für die Übertragung elektronischer Verschlusssachen aktuell noch nicht zugelassen.« Man einigt sich auf eine Verschlüsselungs-Software. Laut Handreichung handelt es sich dabei lediglich um eine Zwischenlösung, bis das Berliner Landesnetz für VS-NID ertüchtigt ist.«



Derselbe Doc. Neues Format.



Kanal entdecken →

Editorial



Karl Fröhlich
Chefredakteur
speicherguide.de

STORAGE 2027: DIE ZEITEN BILLIGER SPEICHER SIND VORBEI

Storage war schon einmal einfacher. Kapazitätsbedarf ermitteln, Leistungsdaten vergleichen, Angebote einholen – und nach drei Jahren war die nächste Generation schneller, größer und günstiger. Mit dieser Erwartung sollten IT-Verantwortliche besser nicht ins Jahr 2027 gehen.

Der KI-Boom verändert den Speichermarkt. Hersteller und Hyperscaler investieren Milliarden, DRAM und Flash werden teurer, Lieferzeiten länger und verbindliche Angebote schwieriger. Falls Sie auf sinkende Preise spekulieren, »vergessen Sie es«.

Blöderweise steigen gleichzeitig die Anforderungen: Speicher soll KI-Anwendungen versorgen, Cyberangriffe überstehen, regulatorische Vorgaben erfüllen und neue Abhängigkeiten vermeiden. Und das nicht für ein Quartal, sondern für fünf bis sieben Jahre. Wer allein auf den Preis pro TByte schaut, rechnet zu kurz.

Das gilt besonders für Storage-as-a-Service. Miet- und Verbrauchsmodelle versprechen Flexibilität und weniger Kapitalbindung. Das kann sinnvoll sein. Wirtschaftlicher wird eine Infrastruktur aber nicht automatisch, nur weil die Rechnung monatlich kommt. Und wer die Hardware nicht besitzt, sollte umso genauer wissen, wer administrativen Zugriff hat, welche Betriebsdaten das Unternehmen verlassen und was am Vertragsende passiert.

Digitale Souveränität lässt sich nicht als Zusatzoption bestellen. Sie muss in Architektur und Verträgen verankert sein.

Auch beim Thema Cyber-Resilienz hilft kein blindes Vertrauen in Herstellerfolien. Unveränderbare Backups sind wichtig. Entscheidend ist jedoch, ob sich die Daten nach einem Angriff schnell und zuverlässig wiederherstellen lassen. Ein Backup allein bringt noch keinen Betrieb zurück.

In der aktuellen Ausgabe blicken wir deshalb auch auf die langfristigen Folgen heutiger Entscheidungen: für Kosten, Sicherheit, KI und die Kontrolle über die eigene Infrastruktur. Denn beim Storage-Einkauf entscheidet nicht allein der Preis, sondern auch, wer langfristig die Kontrolle über die Daten behält.

Ihr Karl Fröhlich
Chefredakteur, speicherguide.de



Der weltweite Enterprise-Storage-Markt wächst zweistellig – vor allem wegen höherer Preise. KI-Rechenzentren binden Produktionskapazitäten, Enterprise-SSDs und Nearline-HDDs bleiben gefragt. Für 2027 zeichnet sich trotz nachlassender Wachstumsraten kaum Entspannung ab. Unternehmen müssen mit hohen Kosten, eingeschränkter Auswahl und unsicheren Lieferbedingungen planen.

Digitale Souveränität und
Storage-Beschaffung

**EIGENTUM, KONTROLLE UND
US-RECHTSRISIKEN**



SEITE
6

Datenspeicherung folgt
dem Workload

**NICHT JEDER EDGE BRAUCHT
EIGENEN STORAGE**



SEITE
26

Editorial	3
Inhalt/Impressum	4

Infrastruktur

Storage-Trends: Mehr Umsatz, weniger Speicher	5
Eigentum, Kontrolle und US-Rechtsrisiken	6
Storage-Anbieter	11
Storage 2027: Beschaffung wird schwieriger, Planung wichtiger	12

Advertorial

Lokale KI, die antwortet und Aufgaben erledigt	16
Objektspeicher auf Tape: Nicht jede Architektur überzeugt	18
NAS zwischen Backup, Archiv und Cyber-Resilienz	20
OSL UVE integriert Compute, Storage und Netzwerk	22

Datenspeicherung

Nicht jeder Edge braucht eigenen Storage	26
---	-----------

Cybersicherheit

KI verändert die Spielregeln der Cybersicherheit	31
---	-----------

Infrastruktur

Wenn das Budget nicht mehr reicht	35
-----------------------------------	-----------

Übersicht Storage-Anbieter



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:
Karl Fröhlich, Uli Neiss
Schlussredaktion:
Karl Fröhlich

Titelbild:
KI-generiert mit DALL-E, speicherguide.de

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. 0177-8487001
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.

Ausblick Storage-Markt 2027

MEHR UMSATZ, WENIGER SPEICHER

Der weltweite Enterprise-Storage-Markt wächst zweistellig – vor allem wegen höherer Preise. KI-Rechenzentren binden Produktionskapazitäten, Enterprise-SSDs und Nearline-HDDs bleiben gefragt. Für 2027 zeichnet sich trotz nachlassender Wachstumsraten kaum Entspannung ab. Unternehmen müssen mit hohen Kosten, eingeschränkter Auswahl und unsicheren Lieferbedingungen planen.



Karl Fröhlich
speicherguide.de

Die Zahlen zeigen das neue Normal: Laut **IDC** stieg der weltweite Umsatz mit externen Enterprise-Storage-Systemen im zweiten Quartal 2026 um 33,7 Prozent auf 10,3 Milliarden US-Dollar. Für das Gesamtjahr erwartet das Marktforschungsunternehmen ein Plus von 22,8 Prozent. Die ausgelieferte Speicherkapazität soll dagegen sinken. Die Anbieter nehmen also mehr ein, obwohl sie weniger Kapazität verkaufen.

Speicher wird zum Engpass

Hyperscaler sichern sich große Speicherkontingente für KI-Rechenzentren durch langfristige Verträge. Für andere Käufer bleibt weniger Auswahl. Besonders gefragt sind Enterprise-SSDs: **TrendForce** erwartet 2026 ein Nachfrageplus von über 80 Prozent, gemessen an der Speicherkapazität. Neben dem Training großer Sprachmodelle steigert der laufende KI-Betrieb den Bedarf an schnellem Speicher. Kleinere Käufer haben dadurch schlechtere Karten bei Preis und Verfügbarkeit.

In Rechenzentren gewinnen hochkapazitive QLC-SSDs an Bedeutung.

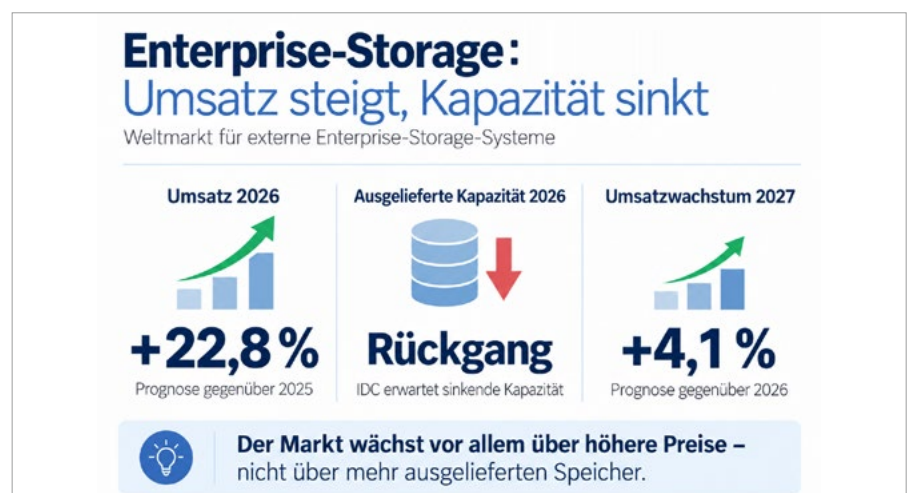
Gleichzeitig bleiben Nearline-HDDs gefragt. Begrenzte Fertigungskapazitäten und die Umstellung auf HAMR erschweren die Versorgung. Flash ersetzt Festplatten deshalb nicht überall. Für große Datenmengen zählen weiterhin Kapazität, Geschwindigkeit und Kosten. Gerade für Archive und Backups bleiben HDDs wirtschaftlich interessant.

Wachstum ohne Entspannung

Trendforce erwartet für das vierte Quartal 2026 um zehn bis 15 Prozent höhere Vertragspreise für konventionelles DRAM und um 15 bis 20 Prozent für NAND-Flash, jeweils gegenüber dem Vorquartal. Bei Enterprise-SSDs sollen die Preise um 23 bis 28 Prozent steigen. Das sind Prognosen für Vertragsmärkte, keine Preisaufschläge, die sich direkt auf komplette Storage-Systeme übertragen lassen. Auch 2027 ist kaum Entspan-

nung in Sicht. IDC erwartet bei externen Enterprise-Storage-Systemen zwar nur noch 4,1 Prozent Umsatzwachstum. Die Preise sollen aber mindestens bis in die zweite Jahreshälfte hoch bleiben. Gartner rechnet bei NAND-Flash mit einem Angebotsdefizit von fünf Prozent und weiteren Preissteigerungen. Zusätzliche Fertigungskapazitäten könnten den Markt ab 2028 stabilisieren. Niedrigere Preise folgen daraus nicht automatisch.

Mittelständische IT-Abteilungen müssen ihren Speicherbedarf daher früher planen. Wer erst bestellt, wenn die Systeme voll sind, riskiert Lieferverzögerungen oder muss eine andere Konfiguration wählen. Deshalb sollten IT-Verantwortliche ihren Bedarf prüfen, Reserven einplanen und lieferbare Alternativen vergleichen. Dabei gehört auch eine unbequeme Frage auf den Tisch: Brauchen wir die geplante Kapazität überhaupt? ■



Der Umsatz mit externen Enterprise-Storage-Systemen soll 2026 um 22,8 Prozent wachsen, obwohl die ausgelieferte Kapazität sinkt.

Digitale Souveränität und Storage-Beschaffung

EIGENTUM, KONTROLLE UND US-RECHTSRISIKEN

Ein Storage-System im eigenen Rechenzentrum ist nicht automatisch souverän. Neben dem Datenstandort zählen Eigentum, Zugriffsrechte und vertragliche Abhängigkeiten. Gerade bei Storage-as-a-Service sollten Unternehmen prüfen, wer die Infrastruktur kontrolliert und was nach Vertragsende geschieht.



Bild: KI-generiert mit DALL-E, speicherguide.de

Ein Storage-System steht im eigenen Rechenzentrum, beispielsweise in München. Die Daten verlassen das Gebäude nicht, die Zugriffe sind abgesichert und die Laufwerke verschlüsselt. Trotzdem gehört die Hardware möglicherweise einem amerikanischen Hersteller. Dieser übernimmt Teile der Administration, erhält Telemetriedaten und verfügt über vertraglich geregelte Fernzugriffsmöglichkeiten.

Ist das souveräne IT?

Ein europäischer Betriebsstandort allein reicht dafür nicht aus. Entscheidend ist, wer die Infrastruktur besitzt, wer darauf zugreifen kann und welche Abhängigkeiten bestehen.

Die Frage wird zunehmend wichtiger, weil Unternehmen ihre Infrastruktur nicht mehr ausschließlich kaufen. Mit Angeboten wie Dell APEX, Net-

App Keystone und Everpure Evergreen//One übertragen sie das nutzungsabhängige Cloud-Modell auf Storage-Systeme im eigenen Rechenzentrum. Das kann wirtschaftlich und betrieblich attraktiv sein. Unter Souveränitäts-Gesichtspunkten entsteht allerdings eine zusätzliche Ebene, die beim klassischen Hardware-Kauf so nicht vorhanden sein muss.

Storage-Beschaffung – vier Modelle im Vergleich			
Eigentum, Kontrolle, Abhängigkeiten und Exit-Fähigkeit auf einen Blick			
1. Kauf Eigene Hardware	2. Subscription Eigene Hardware, nutzungsabhängige Services	3. Storage-as-a-Service Vom Anbieter verwaltete Systeme (z.B. NetApp Keystone, Dell APEX, Everpure Evergreen//One)	4. Abgeschotteter Betrieb z. B. Dark Sites
			
 Eigentum beim Kunden	 Eigentum beim Kunden	 Eigentum meist beim Anbieter oder Finanzierungspartner	 Eigentum je nach Modell (kauf- oder servicebasiert)
 Betrieb weitgehend selbst organisierbar	 Betrieb eigene Hardware, herstellerabhängige Software/Services	 Betrieb vom Anbieter verwaltet	 Betrieb stark eingeschränkt oder isoliert
 Herstellerzugriff je nach Produkt deaktivierbar	 Herstellerzugriff vertraglich geregelt, häufig erforderlich	 Herstellerzugriff Telemetrie und Fernwartung i. d. R. Bestandteil des Services	 Herstellerzugriff nur begrenzt, spezielle Vereinbarungen
 Laufende Kosten Wartung und Support	 Laufende Kosten softwarebasierte Services und Lizenzen	 Laufende Kosten Kapazität und vereinbarte Services	 Laufende Kosten oft zusätzliche Leistungen, eingeschränkte SLAs
 Exit Hardware bleibt, Weiterbetrieb möglich	 Exit Lizenzwechsel möglich, Hardware bleibt	 Exit Datenmigration und Rückgabe der Systeme, vertragliche Pflichten	 Exit abhängig vom Vertrag, Migrationsaufwand möglich
 Höchste Kontrolle und Flexibilität	 Mehr Flexibilität bei kontrollierter Abhängigkeit	 Höhere Abhängigkeit – Exit frühzeitig planen	 Mehr Abschottung, aber nicht ohne Einschränkungen
 Mehr Kontrolle		 Mehr Abhängigkeit	

Kauf, Subscription, Storage-as-a-Service und abgeschotteter Betrieb unterscheiden sich bei Eigentum, Herstellerzugriff und Abhängigkeiten.

US-Jurisdiktion bleibt ein Risiko

Der US CLOUD Act und Section 702 des Foreign Intelligence Surveillance Act (FISA) gehören zu den rechtlichen Rahmenbedingungen, die europäische Unternehmen bei der Auswahl amerikanischer IT-Anbieter berücksichtigen müssen. Beide Regelwerke unterscheiden sich in Voraussetzungen, Adressaten und Verfahren. Gemeinsam ist ihnen, dass US-Recht unter bestimmten Bedingungen behördliche Datenzugriffe ermöglichen kann, auch wenn sich betroffene Daten oder Personen außerhalb der Vereinigten Staaten befinden.

Für die meisten mittelständischen Unternehmen dürfte ein solcher Zugriff unwahrscheinlich sein. Das Compliance-Risiko bleibt trotzdem bestehen.

Allein weil einem US-Hersteller ein Storage-Array gehört, können amerikanische Behörden nicht automatisch auf dessen Daten zugreifen. Beim CLOUD Act kommt es insbesondere darauf an, ob der verpflichtete Anbieter die Daten in seinem Besitz, Gewahrsam oder unter seiner Kontrolle hat.

Fehlt dem Anbieter der direkte Zugriff auf die Nutzdaten, ist die rechtliche Problematik dennoch nicht erledigt. US-Behörden können unter den jeweiligen gesetzlichen Voraussetzungen Daten herausverlangen oder technische Unterstützung verlangen. Einer wirksamen Anordnung müsste der betroffene Anbieter grundsätzlich nachkommen und gegebenenfalls vorhandene Zugriffsmöglichkeiten nutzen. Ob er darüber hinaus neue Zugriffswege schaffen müsste, hängt vom jeweiligen Gesetz und Einzelfall

ab. Verschlüsselung, kundeneigene Schlüssel und eingeschränkte Fernzugriffe können das Risiko reduzieren. Die US-Jurisdiktion des Anbieters beiseitigen sie nicht.

Wem gehört die Hardware?

Beim klassischen Storage-Kauf geht das Eigentum an den Kunden über. Er entscheidet grundsätzlich selbst über Betrieb, Netzwerkanbindung und administrative Zugriffe. Je nach Produkt lassen sich Support-Verbindungen deaktivieren oder kontrollieren. Häufig ist auch ein Betrieb ohne dauerhafte Herstellerverbindung möglich.

Beim vollständigen Storage-as-a-Service gehört die Hardware dagegen meist dem Anbieter oder einem Finanzierungspartner. Der Kunde bezahlt für bereitgestellte oder genutzte Kapazität und vereinbarte Services.



Eigentum, Zugriffsrechte, Betrieb und Exit-Fähigkeit bestimmen gemeinsam, wie souverän eine Storage-Infrastruktur tatsächlich ist.

Das kann die Kapitalbindung senken und den Betrieb vereinfachen, schafft aber eine dauerhafte Vertragsbeziehung.

Ein Beispiel ist Netapp Keystone. Nach den veröffentlichten Vertragsbedingungen bleibt Netapp Eigentümer der bereitgestellten Storage-Produkte. Der Kunde darf sie während der vereinbarten Laufzeit nutzen.

Ein Monitoring-Werkzeug erfasst unter anderem Verbrauchs-, Kapazitäts-, Zustands- und Leistungsdaten für Abrechnung und Betrieb.

Nach Vertragsende muss der Kunde die Nutzung einstellen, seine Daten entfernen und die Systeme zurückgeben oder zur Abholung bereitstellen.

Bei einem gekauften Array bleibt die Hardware dagegen im Unternehmen. Es kann das System grundsätzlich auch ohne neuen Wartungsvertrag weiterbetreiben. Einschränkungen bei Firmware, Ersatzteilen und Support sind dennoch möglich.

Telemetrie und Fernwartung gehören auf den Prüfstand

Die Unterschiede betreffen nicht nur das Eigentum: Dell beschreibt für bestimmte von Dell verwaltete *APEX Data Storage Services* eine dauerhafte Verbindung zwischen der Kundeninstallation und den Dell-Management-Systemen. Das *Secure Connect Gateway* übermittelt Telemetriedaten, unterstützt die Überwachung und ermöglicht Fernzugriffe für Diagnose und Fehlerbehebung.

Die technische Dokumentation beschreibt zudem Funktionen, mit denen sich Konfigurationen und Richtlinien der bereitgestellten Systeme verwalten lassen.

Das bedeutet nicht, dass Dell automatisch auf gespeicherte Nutzdaten zugreifen kann. Es zeigt aber, wie eng Hersteller und Kundeninfrastruktur bei einem verwalteten Service verbunden sein können.

Auch Netapp Keystone nutzt Monitoring-Funktionen. Nach der Servicebeschreibung greift das Werkzeug auf Management-Informationen zu, nicht auf die eigentlichen Kundendaten.

Acht Fragen vor dem Storage-Vertrag

1. Wem gehört die Hardware während und nach der Laufzeit?
2. Wer besitzt administrative Zugriffsrechte?
3. Wer verwaltet die Verschlüsselungsschlüssel?
4. Welche Telemetriedaten verlassen das Rechenzentrum?
5. Lassen sich Fernwartung und Herstellerverbindungen abschalten?
6. Welche Leistungen entfallen bei abgeschottetem Betrieb?
7. Welche Pflichten und Kosten entstehen beim Vertragsende?
8. Kann das Unternehmen die Daten ohne Herstellerunterstützung migrieren?

Fernwartungszugriffe sollen sich durch den Kunden genehmigen, überwachen und protokollieren lassen.

Für die Beschaffung bleiben dennoch wichtige Fragen:

- Welche Informationen verlassen das Rechenzentrum?
- Wer besitzt administrative Berechtigungen?
- Können Verbindungen dauerhaft deaktiviert werden? Welche Leistungen entfallen dann?

Everpure bietet für Evergreen//One besondere Regelungen für abgeschottete Umgebungen, sogenannte Dark-Sites. Kunden benötigen dafür ein entsprechendes Zusatzangebot und müssen Nutzungsprotokolle regelmäßig übermitteln. Bei solchen Installationen sind die vertraglichen SLA-Zusagen eingeschränkt.

Technische Abschottung ist also möglich, gehört aber nicht zwangsläufig zum normalen Leistungsumfang.

Unternehmen sollten deshalb auch prüfen, welche Folgen es hat, wenn sie Herstellerverbindungen nicht zulassen.

Drei Beschaffungsmodelle, unterschiedliche Abhängigkeiten

Nicht jedes Subscription- oder Consumption-Angebot ist eine Hardware-miete. Beim klassischen Kauf besitzt

der Kunde die Infrastruktur. Abhängigkeiten bleiben bei Firmware, Ersatzteilen, Wartung und gegebenenfalls Management-Software bestehen.

Bei nutzungsabhängigen Software- und Service-Verträgen kann die Hardware ebenfalls dem Kunden gehören. Laufende Abhängigkeiten betreffen dann vor allem Lizenzen, Abrechnung, Software-Funktionen und Support.

Beim vollständigen Storage-as-a-Service kommen häufig Eigentumsrechte des Anbieters sowie Nutzungs-, Abrechnungs- und Rückgabepflichten hinzu.

Everpure unterscheidet beispielsweise zwischen dem Kaufmodell Evergreen//Forever, Evergreen//Flex mit kundeneigener Hardware und dem vollständigen As-a-Service-Angebot Evergreen//One.

Entscheidend ist deshalb nicht die Bezeichnung des Angebots, sondern die Kombination aus Eigentum, Vertragsrechten, technischer Kontrolle und Ausstiegsmöglichkeiten.

Die Hersteller reagieren auf europäische Anforderungen

Amerikanische Hersteller reagieren zunehmend auf europäische Souveränitäts-Anforderungen. Netapp hat mit Keystone Sovereign eine entsprechende Variante seines Storage-as-a-Service-Modells angekündigt. Dabei geht es unter anderem um Datenstandort, Support, administrative Zugriffe und Telemetrie.

IBM positioniert *Sovereign Core* als Grundlage für Infrastrukturen, bei denen Kunden und regionale Provider mehr operative Kontrolle übernehmen können. Auch die Zusammenarbeit amerikanischer Technologiehersteller mit europäischen Cloud-Providern nimmt zu.

Solche Angebote können Zugriffsrechte begrenzen und die Kontrolle der Kunden stärken.

Die US-Jurisdiktion des Herstellers bleibt jedoch bestehen. Wie weit ein Angebot die tatsächlichen Abhängigkeiten reduziert, müssen verbindliche Verträge und technische Nachweise zeigen. Ein Sovereign-Label allein genügt nicht.

Was kostet Souveränität – und was kosten Abhängigkeiten?

Inzwischen wird die Auseinandersetzung auch wirtschaftlich geführt. Eine vom US-Technologieverband **CCIA Europe** finanzierte Studie des **European Centre for International Political Economy (ECIPE)** beziffert die möglichen Kosten des geplanten europäischen *Cloud and AI Development Act* (CADA) in einem mittleren Szenario auf 115 Milliarden Euro über zehn Jahre.

Rund 80 Milliarden Euro dieser Schätzung beruhen allerdings auf zusätzlichen Anforderungen für private Unternehmen, die bislang nicht beschlossen sind. Mögliche Vorteile durch geringere Abhängigkeiten, bessere Kontrolle und höhere Resilienz berücksichtigt die Studie nicht als Geldwert.

Cloud-Wechsel und Datenmigrationen verursachen Kosten. Für eine vollständige Rechnung gehören aber auch Anbieterbindung, Vertragsrisiken, Exit-Kosten und rechtliche Unsicherheiten auf den Tisch.

Digitale Souveränität gibt es nicht kostenlos. Die Abhängigkeit von einem Anbieter ebenso wenig.

Der Exit entscheidet mit

Bei gekauften Storage-Systemen bleibt die Hardware im Unternehmen. Bei Mietmodellen muss sie nach Vertragsende häufig zurückgegeben wer-

den. Zuvor sind die Daten zu migrieren und sicher zu löschen.

Netapp Keystone regelt diese Pflichten ausdrücklich. Auch Dell sieht für entsprechende Apex-Abonnements Vorgaben zur Datenmigration, Löschung und Rückgabe vor.

Das kann den Kunden unter Zeitdruck setzen. Er muss Ersatz beschaffen, seine Daten übertragen und den laufenden Betrieb während des Wechsels sicherstellen. Zusätzliche Migrationsleistungen sind nicht automatisch Bestandteil des Servicevertrags.

Deshalb sollten IT-Abteilungen den Exit schon vor der Unterschrift planen.

Dazu gehören dokumentierte Datenformate, ausreichende Migrationsfristen, vertraglich zugesicherte Unterstützung und ein geregelter Weiterbetrieb während der Umstellung.

Souveränität beginnt vor der Unterschrift

Aus den veröffentlichten Quartalszahlen lässt sich bislang nicht ablesen, ob amerikanische Storage-Hersteller wegen digitaler Souveränität Geschäft in

Europa verlieren. Weltweit wachsen ihre Infrastruktur- und Service-Umsätze kräftig. Ein wichtiger Treiber sind die enormen Investitionen in KI-Rechenzentren, die sich stark auf die USA konzentrieren. Sie könnten mögliche Schwächen im europäischen Geschäft überdecken. Detaillierte europäische Storage-Umsätze fehlen weitgehend.

Deutlicher erkennbar sind die Veränderungen bei den Angeboten und Beschaffungsanforderungen. Hersteller reagieren mit regionalisierten Services, abgeschotteten Betriebsmodellen und Sovereign-Produkten.

Für IT-Entscheider zählt nicht, wie souverän ein Anbieter sein Produkt bezeichnet. Entscheidend ist, welche Kontrolle nach Vertragsabschluss tatsächlich beim Kunden bleibt.

Dazu gehören Eigentum, administrative Rechte, Datenflüsse und ein geregelter Anbieterwechsel.

Denn auch ein Storage-System im eigenen Rechenzentrum kann dauerhafte technische, wirtschaftliche und rechtliche Abhängigkeiten schaffen. ■

Weiterführende Informationen:

[US-Infrastruktur boomt – doch Europa bleibt eine Blackbox](#)

[Datensouveränität: Vom Cloud-Label zur messbaren Kontrolle](#)

[Digitale Souveränität braucht Exit-Fähigkeit](#)

0

SHD System-Haus-Dresden GmbH
Drescherhäuser 5b, 01159 Dresden
Tel. 03 51/423 20,
Fax 03 51/423 21 00
info@shd-online.de, www.shd-online.de

Interface Systems GmbH
Zwinglistraße 11/13,
01277 Dresden
Tel. 03 51/31 80 90,
Fax 03 51/31 80 933
info@interface-systems.de,
www.interface-systems.de

ACP IT Solutions AG Jena
Prüssingstraße 35, 07745 Jena
Tel. 036 41/28 70,
Fax 036 41/28 72 87
info@godyo.com, www.godyo.com

1

Dialog Computer Systeme GmbH
Helmholtzstraße 2-9, 10587 Berlin
Tel. 030/390 70 90,
Fax 030/391 70 06
info@dcs.de, www.dcs.de

E-Company
Epiphanienviertel 6, 14059 Berlin
Tel. 030/308 83 80,
Fax 030/30 88 38 30
kontakt@ecompany.ag,
www.ecompany.ag

2

IT-Power Services Deutschland GmbH c/o Freiraum Lüneburg UG,
Salzstraße 1, 21335 Lüneburg
Tel. 0152/21 72 25 88
office@it-ps.de, www.it-ps.de

COMLINE Computer + Software-lösungen SE
Barnerstraße 14d, 22765 Hamburg
Tel. 030 921 02 78 00
Fax 040/51 12 11 11
info@comline-se.de,
www.comline-se.de

eSell Nord GmbH
Rotdornwiese 4, 25421 Pinneberg
Tel. 040/228 65 10-0
info@eSell.hamburg,
www.eSell.hamburg

Basys EDV-Systeme GmbH
Hermine-Seelhoff-Straße 1,
28357 Bremen
Tel. 04 21/43 42 030,
Fax 04 21/491 48 33
info@basys-bremen.de,
www.basys-bremen.de

3

DTS Systeme GmbH
Schrewestraße 2, 32051 Herford
Tel. 052 21/101 30 00,
Fax 052 21/101 30 01
info@dts.de, www.dts.de

neam IT-Services GmbH
Technologiepark 8,
33100 Paderborn
Tel. 05251/1652-0
www.neam.de

probusiness Nord GmbH
Berliner Str. 14, 31174 Schellerten
Tel. 05 11/600 66-0,
Fax 05 11/60 06 61 55
nord@probusiness.de,
www.probusiness.de

Netline Computer & Netzwerk-systeme GmbH
Hinter dem Dorfe 16,
37176 Nörten-Hardenberg
Tel. +49 5503 75733-0,
Fax 05 51/507 37 20
www.netline-gmbh.de

PDV-Systeme GmbH
Dörntener Straße 2 A, 38644 Goslar
Tel. 053 21/370 30,
Fax 053 21/37 03 89 24
info@pdv-systeme.de,
www.pdv-systeme.de

4

Cancom GmbH
Elisabeth-Selbert-Str. 1,
40764 Langenfeld
Tel. 02173/5966 0,
www.cancom.de

i-Tech GmbH & Co. KG
Dießener Bruch 114c,
47805 Krefeld
Tel. 021 51/579 95 80,
Fax 021 51/57 99 58 58
info@i-tech24.de, www.i-tech24.de

**Actidata**www.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 Systemhäuser auf das Industrie- und Geschäftskundensegment mit dem Ziel, professionelle Speicherlösungen zu platzieren.

**Fast LTA**www.fast-lta.de**Sitz der Gesellschaft:** München**Niederlassungen in Deutschland:** 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.

**NCS**www.ncs.de**Sitz der Gesellschaft:** Friedberg bei Augsburg**Jahr der Gründung:** 1997**Zielgruppe:** KMUs, Behörden, Kommunen, VARs und Industriekunden

NCS ist ein herstellerunabhängiges IT-Systemhaus für Unternehmen, die ihre IT zuverlässig, sicher und ohne unnötige Komplexität betreiben wollen. Das Team unterstützt bei Beratung, Beschaffung, Umsetzung und laufendem Betrieb – von Clients, Netzwerken und Microsoft 365 über Storage, Backup, Security und Monitoring bis zu Server- und Rechenzentrumsdiensten. NCS ist in Friedberg bei Augsburg, München und Ulm vertreten.

**OSL Gesellschaft für offene Systemlösungen mbH**www.osl.eu**Sitz der Gesellschaft:** Schöneiche bei Berlin**Jahr der Gründung:** 2002**Zielgruppe:** KMU, Großunternehmen, Rechenzentren, Systemhäuser, IT-Dienstleister und öffentliche Einrichtungen

OSL entwickelt betriebssystemnahe Infrastruktur-Software auf der Basis einer eigenen integrierten Speichervirtualisierungs- und Cluster-Technologie. Mit OSL Storage Cluster und OSL Unified Virtualisation Environment unterstützt das Unternehmen den zuverlässigen Betrieb geschäftskritischer Speicher- und Virtualisierungs-Umgebungen. Im Mittelpunkt stehen einfache Administration, Ausfallsicherheit, Skalierbarkeit, Portabilität sowie Unabhängigkeit von spezifischer Hardware.

**PoINT Software & Systems GmbH**www.point.de**Sitz der Gesellschaft:** Siegen**Jahr der Gründung:** 1994**Zielgruppe:** Mittelstand, Großunternehmen, Rechenzentren, Cloud- und Storage-Provider, Systemintegratoren und VARs

PoINT Software & Systems entwickelt Lösungen für Datenmanagement, Archivierung und die effiziente Nutzung unterschiedlicher Speichertechnologien. Das Portfolio umfasst u.a. Software für Storage-Tiering, Object-Storage und S3-to-Tape-Architekturen. Unternehmen und Service-Provider können damit Daten wirtschaftlich speichern, langfristig archivieren und Compliance-Anforderungen erfüllen.

**RNT Rausch / Pyramid Computer GmbH**www.rnt.de**Sitz der Gesellschaft:** Freiburg i. Breisgau (Pyramid Computer GmbH)**Weitere Standorte:** Ettlingen (RNT), Ichttershausen, Witzzenhausen**Jahr der Gründung:** 1985 (Pyramid), 1998 (RNT Rausch)**Zielgruppe:** KMU, Großunternehmen, Rechenzentren, Cloud- und Service-Provider, Systemintegratoren, VARs und Industriekunden

RNT Rausch und Pyramid Computer bündeln ihre Kompetenzen in der Entwicklung und Fertigung leistungsfähiger Server- und Storage-Systeme Made in Germany. Das Portfolio umfasst skalierbare Speicherlösungen, Software-Defined Storage, S3-Object-Storage und Immutable-Backup-Appliances sowie Infrastrukturen für Hybrid-Cloud und lokale KI.

Interview mit Patricia Hillebrand, Business Development Manager, Pyramid Computer

STORAGE 2027: BESCHAFFUNG WIRD SCHWIERIGER, PLANUNG WICHTIGER

Lieferzeiten steigen, Preise schwanken und Wunschkonfigurationen sind nicht immer verfügbar. Gleichzeitig erhöhen KI, Cyber-Resilienz und digitale Souveränität die Anforderungen an Storage. Wir sprachen mit Patricia Hillebrand, Business Development Manager bei Pyramid Computer, über die aktuelle Beschaffungslage, neue Prioritäten beim Storage-Einkauf und die passende Architektur für 2027.



Lieferzeiten werden länger, Preise schwanken und Wunschkonfigurationen sind nicht immer verfügbar. Wie schwierig ist es derzeit überhaupt, Storage-Systeme planbar zu beschaffen?

Hillebrand: Extrem herausfordernd. Unser Einkaufsteam läuft jeden Tag zu neuer Hochform auf und holt aus den exzellenten bestehenden Beziehungen mit unseren Herstellern und der Distribution alles heraus. Parallel dazu suchen wir weitere Quellen. Von der vertrieblichen Seite her gehen wir proaktiv auf Kunden und Partner zu mit der Information, was aktuell aus Lagerbeständen verfügbar ist.

Viele haben bereits verstanden, dass eine Wunschkonfiguration mit teilweise extremen Lieferzeiten und fehlender Preisgarantie verbunden ist. Nicht

weil wir unsere Kunden abzocken, sondern weil auch wir von den Herstellern keine verbindlichen Termine oder Preise mehr bekommen. Deshalb setzen wir wo möglich auf schlüsselfertige Plug&Play-Appliances. Wir bestimmen die Konfiguration, die immer optimal zum Beispiel auf die Objektspeicher-Software abgestimmt ist. Von welchem Hersteller am Ende des Tages verbaute Komponenten sind, bestimmen wir.

Alles kommt von führenden Herstellern in Enterprise Qualität und ist durchgetestet, aber wir entscheiden und nehmen, was wir kriegen können. Nur so sind wir in der Lage, Preise in eine verbindliche Auftragsbestätigung zu schreiben, auf die sich unsere Kunden und Partner auch verlassen können.

Verführt diese Situation Unternehmen nicht dazu, kurzfristig nach Verfügbarkeit und Preis zu entscheiden – obwohl Storage für viele Jahre ausgelegt wird?

Hillebrand: Wir befinden uns aktuell im 4. Quartal und müssen daher natürlich mit der Situation umgehen, dass existierende Budgets jetzt noch schnell vor dem Ende des Kalenderjahres ausgegeben werden müssen. Wer sich in einer solchen Situation befindet, läuft definitiv in Gefahr, sich von einer falschen Entscheidung verleiten zu lassen. Es gibt immer noch Entscheider, die trotz aller Hinweise und

Warnungen weiter gepokert und darauf spekuliert haben, dass die Blase platzt und wir eine Normalisierung sehen bei Preisen und Verfügbarkeiten.

Wenn ein Storage-System fünf bis sieben Jahre laufen soll, kann »Was ist heute verfügbar und günstig?« kein ernsthaftes Beschauungskriterium sein. Wer Storage nur nach Tagespreis und Lagerbestand kauft, optimiert möglicherweise kurzfristig den Kauf, aber ersetzt strategisches Denken und Handeln durch operative Hektik. Mit einer gehörigen Portion Glück kann das gut gehen, aber das Risiko ist hoch, dass ein auf diesem Weg beschafftes Storage-System nicht geeignet ist und am Ende des Tages entweder den Betrieb verteuert oder die Wettbewerbsfähigkeit des Unternehmens einschränkt. Wir haben uns für einen goldenen Mittelweg entschieden und bieten als Kompromiss ausgewählte Appliances mit modernem Objektspeicher als schlüsselfertige Komplettlösung an, die kurzfristig lieferbar und keine Mogelpackung sind.

Kurzfristige Beschaffung darf langfristige Planung nicht ersetzen

Server lassen sich ersetzen, Anwendungen migrieren – die Daten bleiben. Warum ist Storage das Fundament des modernen IT-Stacks?

Hillebrand: Server kannst Du ersetzen, Anwendungen migrieren und Cloud-Ressourcen flexibel buchen oder austauschen. Daten dagegen sind das Ergebnis von Jahren, wenn nicht Jahrzehnten: Für jedes Unternehmen unverzichtbare Daten lassen sich nicht einfach neu installieren – du kannst sie entweder verarbeiten, bewahren und schützen oder verlieren. Deshalb ist Storage nicht irgendeine Komponente im IT-Stack – es ist das Fundament, auf dem alles Weitere basiert.

Wer also heute die großen Themen in der IT ernst nimmt – und das ist nicht auf KI beschränkt – muss sich in erster Linie damit beschäftigen, wo die wertvollen Daten liegen, wer sie kontrolliert und wie sicher sie dort sind. Deshalb ist Storage viel mehr als nur eine Kostenstelle, sondern das Gedächtnis eines jeden Unternehmens – egal ob Mittelstand oder Großkonzern.

Das heißt, Storage ist heute weit mehr als die Wahl zwischen HDD, Flash und Preis pro TByte. Für viele klingt es aber auf den ersten Blick nach einer klar definierten Produktkategorie, mit Commodity-Potenzial.

Hillebrand: Wenn wir uns rein auf die Hardware-Ebene und den ersten Blick beschränken, stimme ich zu. Aber die Zeiten sind vorbei, in denen es vollkommen ausgereicht hat, Storage nach HDD vs. All-Flash und Preis pro TByte auszuwählen.

Storage ist komplex, weil Daten nicht gleich Daten sind. Du hast strukturierte und unstrukturierte Daten, Backup, Archiv, klassische sowie unternehmensspezifische Anwendungen, Datenbanken und jetzt auch noch KI – die Storage-Architektur muss die unterschiedlichen Anforderungen an Leistung, Verfügbarkeit, Skalierbarkeit, Sicherheit und natürlich auch Kosten adressieren.

Storage ist komplex, weil Du darüber hinaus auch Datenwachstum und zukünftige Anwendungen mitdenken musst. Storage entscheidet über die Verfügbarkeit von Daten, vor allem nach einem Cyberangriff. Moderne Storage-Architektur bedeutet, Daten intelligent zu platzieren – und sie ge-



Bild: KI-generiert mit DALL-E, speicherguide.de

Objektspeicher eignet sich besonders für große Mengen unstrukturierter Daten und bildet eine skalierbare Basis für KI, Analytics und Data-Lakes. Für extrem latenzkritische Workloads sowie klassische Block- und File-Zugriffe bleiben andere Storage-Technologien sinnvoll.

nau dann verfügbar zu machen, wenn man sie braucht.

Wer Storage immer noch als Commodity sieht, zahlt früher oder später drauf bei Betrieb und Risiko. Ich gehe sogar noch einen Schritt weiter: Storage ist weitaus mehr als Hardware. Storage ist die Infrastruktur, auf der der Wert eines jeden Datensatzes überhaupt erst entsteht.

Storage ist längst mehr als Hardware und Kapazität

KI wird häufig als Server- oder GPU-Thema diskutiert. Warum ist KI in Wahrheit mindestens genauso sehr ein Storage-Thema?

Hillebrand: KI wird gerne als GPU- oder Server-Thema betrachtet, es macht ja auch Spaß darüber zu fachsimpeln. Aber KI ist in erster Linie ein Datenthema, denn die neueste und teuerste GPU bringt wenig, wenn die Daten nicht schnell, zuverlässig und im richtigen Format für die Verarbeitung verfügbar sind.

Grundsätzlich gilt: Je größer die Datenmengen und je komplexer die Modelle werden, desto wichtiger ist eine moderne Storage-Technologie, die für eine moderne digitale Welt gemacht ist. Ein solcher Speicher stellt sicher, dass KI-Modelle auf große Datenbestände zugreifen, Trainingsdaten effizient verarbeiten und die Ergebnisse wieder speichern, um sie für weitere Anwendungen nutzen können.

Gerade unstrukturierte Daten sind dabei ein wichtiger Rohstoff für jede KI und müssen deswegen skalierbar, sicher und jederzeit verfügbar sein. Wer bei KI also nur über Compute spricht, baut zwar einen Rennwagen, fährt aber mit großer Wahrscheinlichkeit nur auf einem holprigen Feldweg. Und wer bei KI nur in Compute investiert, riskiert, dass teure Rechenleistung auf die Daten wartet. Eine moderne Storage-Architektur sorgt dafür, dass Daten dort verfügbar sind, wo KI sie braucht – und macht aus Rechenleistung tatsächlich nutzbare KI-Leistung.

Objektspeicher wird zur Plattform für unstrukturierte Daten

Objektspeicher ist technisch längst etabliert. Warum ist er im Mittelstand trotzdem noch nicht selbstverständlich?

Hillebrand: Das frage ich mich auch, denn die Technik ist längst reif und die Vorteile sind so offensichtlich. Wahrscheinlich ist es eine Mischung aus konservativen Herangehensweisen, veralteten Gewohnheiten, Altlasten und Missverständnissen.

Viele traditionell im Einsatz befindliche Anwendungen basieren auf File- oder Block-Protokollen. Cloud-Applikationen wie auch die Cloud selber sprechen aber S3. Das hört sich erst einmal wie ein Widerspruch an, ist aber keiner, denn im Markt gibt es inzwischen hervorragende Lösungen und Gateways, die Block, File und S3 zusammenbringen.

Ein weiterer Grund ist vermutlich der hartnäckige Mythos, dass Objektspeicher zwar günstig aber langsam ist und deshalb vor allem geeignet für Backups oder kalte Daten aber nicht anderes. Dieser Mythos ist leider immer noch weit verbreitet, obwohl gerade All-Flash-Objektspeicher heute hohe Durchsätze für Trainingsdaten, Data-Lakes und Analytics liefert. Selbst HDD-basierter Objektspeicher kann für Inference-Prozesse vollkommen ausreichend sein, wenn zum Beispiel die Netzwerkkapazität nur 10GbE beträgt.

S3 ist zwar aus der Public-Cloud bekannt, viele IT-Teams haben aber noch nie einen Objektspeicher selbst betrieben. Buckets, Erasure-Coding, Lifecycle-Regeln oder Object-Lock sind neu und die Storage-Admins der klassischen SAN-Welt haben andere Schwerpunkte. Was Du nicht kennst, kannst Du nicht administrieren und so wird Object-Storage ohne entsprechende Aus- und Weiterbildung weiterhin im Produktivbetrieb fehlen.

Das wird nicht lange gut gehen, denn Trainingsdaten, Dokumentenbestände, Logs und Sensordaten sind unstrukturiert, riesig und wachsen

schnell. Genau dafür ist Objektspeicher gebaut. Hinzu kommen Souveränitätsanforderungen, die eine eigene, europäisch kontrollierte hybride Datenhaltung – vor Ort und in einer europäischen Cloud – erfordern. Wer Objektspeicher immer noch als Ausnahme betrachtet, wird über kurz oder lang den Anschluss im KI-Zeitalter verlieren.

Was macht Objektspeicher gerade für KI-Workloads interessant und wo stößt er an Grenzen?

Hillebrand: Objektspeicher als zentrale Datenplattform adressiert die größte

Herausforderung im KI-Bereich: riesige und stetig weiterwachsende Mengen von unstrukturierten Daten. Er ist dank Object-Lock unveränderbar, lässt sich nahezu beliebig skalieren, bietet über die S3-Schnittstelle einen offenen Zugriff und de-facto Standard. Im Vergleich mit anderen Storage-Technologien punktet Object-Storage durch niedrige Gesamtbetriebskosten und kann Daten für unterschiedlichste Anwendungen inklusive KI-Workloads zentral verfügbar machen. Damit wird Objektspeicher vom klassischen Archiv zum strategischen Daten-Pool. Aber

Storage-Einkauf 2027

Zwischen Beschaffungsdruck und langfristiger Planung



Bild: KI-generiert mit DALL-E, speicherguide.de

auch Objektspeicher ist kein Allheilmittel. Wo extrem niedrige Latenzen, sehr viele kleine I/O-Operationen oder klassische Block- und Dateisystemzugriffe gefragt sind, haben andere Storage-Technologien weiterhin ihre Berechtigung. Die Zukunft der IT ist nicht schwarz oder weiß, sondern besteht aus den richtigen Kombinationen: Block, File und Object Storage, Daten in einer europäischen Cloud und On-Prem – immer dort, wo sie je nach Anwendungsfall und -umgebung technisch sowie wirtschaftlich Sinn ergeben.

Cloud, On-Premises oder Hybrid: Nach welchen Kriterien sollte ein Unternehmen heute entscheiden, wo seine Daten liegen?

Hillebrand: In unserem digitalen Zeitalter sind Entscheidungen zwischen »entweder« oder »nicht mehr zielführend«. Unterschiedliche Workloads, wachsende Datenmengen, KI, Cyberbedrohungen, regulatorische Anforderungen, das verständliche Streben nach digitaler Souveränität und weniger Abhängigkeiten in Europa, usw. sprechen ganz klar für hybride Ansätze. Dazu kommen Skalierbarkeit, Energieeffizienz, Kosten und die Frage, wer die Kontrolle über die Daten behält. Die Herausforderung ist daher nicht, Daten einfach nur zu speichern, sondern sie so zu speichern, dass sie heute funktionieren und morgen neue Möglichkeiten eröffnen.

Beim Storage-Einkauf zählen die Folgen über Jahre

Preis, Kapazität und Performance sind leicht vergleichbar. Welche Kriterien entscheiden über einen guten Storage-Einkauf – und werden trotzdem häufig unterschätzt?

Hillebrand: Wenn wir uns darauf einigen, dass Daten das wertvollste Gut eines Unternehmens sind, dann darf Storage nicht länger nach alten Kriterien wie Preis, Kapazität und IOPS und Komfortzonen der IT-Mannschaft beschafft werden. Viel wichtiger ist die Frage, wie groß meine Datenmenge in drei bis fünf Jahren sein wird und was

mit diesen Daten in diesem Zeitraum und darüber hinaus passieren soll. Storage ist das strategische Fundament eines jeden IT-Stacks, auf dem die Wertschöpfungskette der Unternehmensdaten beginnt.

Papier ist geduldig, teuer wird es oft bei dem, was nicht im Datenblatt oder nur im Hochglanzprospekt steht. Ist der Speicher wirklich unveränderbar oder eher eine Mogelpackung? Was kostet eine Erweiterung nach drei Jahren? Brauche ich eine All-Flash-Lösung oder reichen Festplatten aus? Woher kommt die Hardware, kann der Anbieter verlässlich liefern? Wie steht es um Energieverbrauch, Gesamtbetriebskosten, Cyber-Resilienz, Compliance und Herstellerabhängigkeit?

Viel wichtiger als die Frage nach den Kosten per TByte ist die klare Definition des Anwendungsfalls: Was brauche ich heute, was in fünf bis sieben Jahren und wie flexibel, sicher und wirtschaftlich ist diese Architektur über diesen langen Zeitraum hinweg betrachtet. Storage kaufst Du heute, die Konsequenzen dieser Entscheidung trägt jedes Unternehmen aber mindestens ein halbes Jahrzehnt oder länger.

Wo ist ein mittelständischer Hersteller gegenüber den großen Konzernen im Nachteil – und wo im Vorteil?

Hillebrand: Unsere Abnahmemengen sind größer als es scheint, wenn man auf einen mittelständischen Hardwarehersteller mit Hauptsitz in Freiburg schaut. Zu unseren internationalen Kunden gehören namhafte Weltmarken aus ganz unterschiedlichen Branchen, die unsere Lösungen hinter verschlossenen Türen in ihren Rechenzentren stehen haben oder als ODM/OEM Lösung in den Markt bringen. So kommen wir auf Abnahmemengen, die Komponentenhersteller ernst nehmen – es steht nicht immer Pyramid drauf, wo Pyramid drin ist. Ein



weiterer nicht zu unterschätzender Vorteil ist, dass wir mit eigenem Personal in Deutschland vor Ort an einem unserer 4 Standorte fertigen und somit selber entscheiden, was wir verbauen. Dabei halten wir uns natürlich strikt an HCLs und Hardware-Vorgaben von ISVs. Einzige Ausnahme sind dedizierte Kundenvorgaben. Aber auch in diesem Fall können wir agil und flexibel reagieren: Wenn Plan A nicht funktioniert, gehen wir proaktiv auf unsere Kunden und Partner zu und schlagen einen Plan B vor.

Nicht zu vernachlässigen ist ein weiteres Alleinstellungsmerkmal, denn wir liefern souveräne Hardware-Lösungen Made in Germany inklusive Service- und Support-Dienstleistungen, die ebenfalls von realen Kollegen aus Freiburg, Ettlingen oder Witzenhäusern durchgeführt werden.

Welchen Rat würdest Du einem IT-Leiter für seine Storage-Planung 2027 geben?

Hillebrand: Storage 2027 muss wertvolle Unternehmensdaten verfügbar, sicher, skalierbar und langfristig kontrollierbar machen. Das gilt nicht nur für KI, sondern auch für viele neue Workloads. Genau deshalb wird die Wahl der Storage-Architektur zu einer strategischen Unternehmensentscheidung. Objektspeicher gehört in jedes Rechenzentrum – oder für kleinere Datenmengen als schlüsselfertige Appliance, in jeden Server-Raum. ■

On-Premises-KI: Von der KI-Suche zur vollwertigen KI-Arbeitsumgebung

LOKALE KI, DIE ANTWORTET UND AUFGABEN ERLEDIGT

Ihre Mitarbeiter arbeiten längst mit KI – häufig über Dienste, die niemand freigegeben hat. Ein Verbot hält das kaum auf, und eine Cloud-Lizenz verlagert vertrauliche Inhalte zu fremden Anbietern. Gefragt ist eine KI, die wiederkehrende Aufgaben so selbstverständlich erledigt wie die großen Dienste, dabei im eigenen Rechenzentrum bleibt und das zu kalkulierbaren Kosten.



Roland Stritt
FAST LTA

Es ist Donnerstagnachmittag in einem mittelständischen Maschinenbauunternehmen irgendwo zwischen Ulm und Augsburg. Die Leiterin des Vertragsmanagements hat einen 40-seitigen Liefervertrag eines Großkunden auf dem Tisch, Antwortfrist Montag. Sie weiß, was zu tun ist: Haftungsklauseln gegen die hauseigenen Vorgaben prüfen, Abweichungen markieren, Gegenvorschläge formulieren, dazu die Liefertermine mit dem ERP abgleichen. Zwei Tage Arbeit, wenn nichts dazwischenkommt.

Am Wochenende hat sie zu Hause gesehen, wie schnell ein Cloud-Chatbot so etwas erledigt. Die Versuchung ist groß, den Vertrag einfach hochzuladen. Sie tut es nicht, weil sie weiß, dass Kundenverträge das Haus nicht verlassen dürfen. Ob alle in ihrer Abteilung ebenso konsequent sind, weiß sie allerdings nicht.

Die Belegschaft ist schneller als die Freigabe

Die Szene spielt sich so oder ähnlich in vielen Unternehmen ab. Wer abends

mit einem großen KI-Dienst einen Brief entwirft oder eine Reise plant, erwartet am nächsten Morgen im Büro denselben Komfort. Gibt es dort kein freigegebenes Werkzeug, entsteht Schatten-KI: Verträge, Konstruktionsdaten oder Personalvorgänge landen in privaten Konten, ohne dass die IT davon weiß.

Für IT-Leiter und Datenschutzbeauftragte ist das ein Dilemma. Ein Verbot treibt die Nutzung weiter in den Untergrund. Eine Unternehmenslizenz bei einem Cloud-Anbieter bringt den Komfort zurück, legt die Inhalte aber in fremde Rechenzentren, oft unter US-Recht, und die Abrechnung nach Token wächst mit jeder Nutzung. Lokale Suchsysteme halten die Daten im Haus und beantworten Fragen zuverlässig. Den Entwurf, die Auswertung oder den Abgleich mit dem ERP erledigt danach jedoch weiterhin der Mensch.

Das erleben wir bei **FAST LTA** auch selbst. Seit dem Frühjahr 2026 führen wir *Silent AI* bei Interessenten und auf Messen vor. Die Software beantwortet Fragen aus den eigenen Dokumenten, mit Quellenverweis und unter Wahrung der Zugriffsrechte, die aus dem Active-Directory und den angebundenen Quellsystemen synchronisiert werden. Trotzdem fällt nach fast jeder Vorführung derselbe Satz: »Kann es mir das auch gleich erstellen?«

Von der Frage zur erledigten Aufgabe

Seit Oktober 2026 gibt es mit *Silent AI Pro* eine KI-Arbeitsumgebung, die vollständig im eigenen Rechenzentrum läuft. Im Vertragsmanagement sieht das so aus. Die Leiterin legt ein Projekt an, in dem der Kundenvertrag, die internen Vertragsrichtlinien und die Korrespondenz der letzten Verhandlungsrunde liegen. Der Arbeitsstand bleibt



Silent AI Pro läuft auf einer 4-HE-Appliance mit bis zu drei Nvidia-GPUs. Die Bestückung lässt sich jederzeit erweitern.

erhalten. Sie kann am Freitag dort weitermachen, wo sie am Donnerstag aufgehört hat.

Die Prüfung gegen die Hausvorgaben muss sie nicht jedes Mal neu erklären. Die Rechtsabteilung hat den Ablauf einmal als Skill hinterlegt. Seitdem steht er allen Berechtigten im Unternehmen zur Verfügung. Den mehrstufigen Teil übernimmt ein Agent. Er gleicht die zugesagten Liefertermine über eine Schnittstelle mit dem ERP ab, markiert kritische Klauseln und prüft seine Zwischenergebnisse, bevor er weiterarbeitet. Am Ende steht ein Artefakt, in diesem Fall eine kommentierte Abweichungsliste mit Formulierungsvorschlägen, die sich weiterbearbeiten und an die Geschäftsführung übergeben lässt. Jede Aussage darin verweist auf die Fundstelle im Originaldokument.

Dasselbe Prinzip trägt auch außerhalb der Rechtsabteilung. Ein Servicetechniker kommt von einem Einsatz beim Kunden zurück und lässt seinen Bericht nach dem festen Muster des Hauses erstellen. Der Agent holt dafür die Daten aus dem Ticketsystem, ergänzt die passenden Stellen aus der Maschinendokumentation und legt den Entwurf zur Freigabe vor. Der Techniker prüft, korrigiert, wo nötig, und gibt den Bericht frei.

Agenten mit denselben Rechten wie ihre Nutzer

Wer von »Agenten« hört, denkt schnell an Kontrollverlust. *Silent AI Pro* übernimmt deshalb das Rechtenmodell der Basis unverändert. Die Berechtigungen werden aus dem Active-Directory und den angebundenen Quellsystemen synchronisiert, und das gilt für Agenten genauso wie für Menschen. Rollenbasierte Zugriffskontrolle und Mandantenfähigkeit trennen Abteilungen oder Gesellschaften auf demselben System voneinander. Eine Protokollierung aller Agentenzugriffe macht nachvollziehbar, wer was ausgelöst hat. Das hilft, wenn bei einer Prüfung nach *NIS-2* oder dem *EU AI Act* nachzuweisen ist, welche Aufgabe mit welchen Daten bearbeitet wurde.

Bevor Sie entscheiden: drei Fragen an Ihre KI-Strategie

Wo arbeiten Ihre Mitarbeiter heute schon mit KI? Wer keine freigegebene Lösung anbietet, hat in der Regel bereits eine nicht freigegebene im Haus.

Welche Aufgaben soll die KI selbst erledigen? An Vertragsprüfungen, Serviceberichten oder Recherchen über mehrere Fachsysteme lässt sich ablesen, ob eine Suche reicht oder eine Arbeitsumgebung nötig ist.

Was kostet Ihre KI, wenn sie erfolgreich ist? Bei Token-Abrechnung steigt die Rechnung mit der Nutzung. Feste Kosten machen den Erfolg planbar.

Wir zeigen Ihnen *Silent AI Pro* an Ihren eigenen Dokumenten und Fragestellungen, nicht an einer Demo-Datenbank. Demo anfragen unter

www.fast-lta.de/de/produkte/silent-ai

Bei aktivierter RAG-Funktion arbeitet *Silent AI* annähernd ohne Halluzinationen, jede Antwort trägt einen nachprüfbaren Quellenverweis. Fehlt in den Dokumenten eine belastbare Grundlage, sagt das System das, statt etwas Plausibles zu formulieren.

Feste Kosten statt Taxiuhr

Bei agentischer KI verändert sich auch die Kostenrechnung. Ein Agentendurchlauf verbraucht ein Vielfaches der Rechenleistung einer einzelnen Anfrage. Wer nach Token abrechnet, macht also ausgerechnet die produktivste Nutzung zur teuersten. *Silent AI Pro* wird als Appliance zum Festpreis angeboten, ohne nutzungsabhängige Token- oder API-Gebühren und unabhängig von der Nutzerzahl. Hardware-Erweiterungen und *CARE*-Wartung kommen als planbare Posten hinzu. Das Sprachmodell ist austauschbar, und wer mit einer GPU startet, rüstet bei Bedarf nach, ohne die Appliance zu tauschen.

Souveränität ist kein Zusatzmodul

Die Cloud-Abgrenzung entscheidet sich am Aufstellungsort. Werden Prompts, Dokumente und Ergebnisse ausschließlich im eigenen Netz verarbeitet, entfällt der Datentransfer an einen Cloud-Anbieter. Bleiben auch Betriebs- und Supportzugriffe unter der Kontrolle des Unternehmens, hat kein Anbieter Einblick in die Inhalte,

und niemand kann damit Modelle trainieren. Das senkt zugleich das Risiko aus US-Zugriffsnormen wie *US-CLOUD Act* und *FISA 702* erheblich. Für Unternehmen, die der DSGVO, *NIS-2* oder branchenspezifischen Vorgaben unterliegen, ist das oft die Voraussetzung, KI überhaupt mit sensiblen Daten einzusetzen.

Die Leiterin des Vertragsmanagements hat ihre Abweichungsliste übrigens am Freitagmittag fertig. Am Montag führt sie das Gespräch mit dem Kunden, und das bleibt ihre Aufgabe.

FAST LTA ist ein deutsches Unternehmen mit Entwicklung, Support und Vertrieb in München. Bekannt ist *FAST LTA* für Speichersysteme für Backup und Archivierung, die auch einem Ransomware-Angriff standhalten. Mit *Silent AI* überträgt das Unternehmen dieses Prinzip der Datenhoheit auf künstliche Intelligenz. *CARE*-Wartungsverträge sichern Support und Updates über eine Laufzeit von einem, drei oder fünf Jahren zu festen Konditionen. ■

Weitere Informationen:

FAST LTA GmbH

Tölzer Straße 1, 81379 München
Tel. 089/89 047-0

E-Mail: info@fast-lta.de

www.fast-lta.de/de/produkte/silent-ai

S3-to-Tape: Auswahlkriterien für eine Tape-basierte S3 Object-Storage-Software

OBJEKTSPEICHER AUF TAPE: NICHT JEDE ARCHITEKTUR ÜBERZEUGT

Die Einführung einer Tape-basierten S3-Objektspeicherlösung bietet die Antwort auf die drängenden Herausforderungen im Storage-Bereich. Unternehmen können so den wachsenden Datenmengen und steigenden Sicherheitsanforderungen mit dem Komfort der S3-Schnittstelle und der hohen Wirtschaftlichkeit der Tape-Technologie begegnen. Für eine Kaufentscheidung sind sowohl funktionale als auch herstellerspezifische Kriterien maßgebend.

Für eine Tape-basierte S3-Object-Storage-Software ist entscheidend, welcher architektonische Ansatz zugrunde liegt. Damit die Lösung höchste Effizienz in Bezug auf Datensicherheit, Wirtschaftlichkeit und Skalierbarkeit bietet, muss die Architektur speziell für Tape konzipiert sein.

Architekturen, bei denen ein S3-Service auf ein Datei- oder HSM-System aufgesetzt wird, haben viele Nachteile:

- Dieser Ansatz erfordert eine Zwischenspeicherung auf Festplatten. Dazu wäre zusätzliche Hardware notwendig.
- Eine zusätzliche Dateisystem-Schicht erhöht die Komplexität unnötig.

Der Objektspeicher **PoINT Archival Gateway** wurde speziell für Tape-Loader und -Libraries entwickelt. Die Software schreibt Daten direkt auf Tape-Medien. Ein Caching auf Disk und eine S3-kompatible Disk-Speicherklassen sind optional möglich, eine Zwischenspeicherung auf Festplatten ist jedoch nicht zwingend erforderlich.

Kompatibilität mit Speicherklassen S3 Standard und S3 Glacier

Viele Anwendungen, die Daten über eine S3-Schnittstelle speichern, unterstützen nur die Speicherklassen S3-Standard. Häufig unterstützen Applikationen jedoch keine S3 Glacier-Speicherklassen. PoINT Archival Gateway bietet eine S3-Standard-Spei-



Thomas Thalmann
PoINT Software &
Systems

cherklasse, sodass viele S3-fähige Anwendungen damit Tape als Zielspeicher verwenden können. Optional unterstützt PoINT Archival Gateway auch S3 Glacier.

Flexible Auswahl des Tape-Formats

Das Beschreiben der Tapes kann in unterschiedlichen Formaten erfolgen. Das standardisierte LTFS-Format bietet den entscheidenden Vorteil, dass die Daten später auch unabhängig von der schreibenden Software in einem LTFS-kompatiblen System gelesen werden können.

Proprietäre Formate bleiben auch beim Lesevorgang an die Speicher-Software gebunden. Diesen Vorteil der Unabhängigkeit können sie also nicht für sich geltend machen. Ein optimiertes proprietäres Format kann jedoch eine weiterreichende Funktionalität bieten.

PoINT Archival Gateway stellt beide Optionen bereit: Der Nutzer kann das standardisierte LTFS-Format wählen. Die Datenobjekte sind dann unmittel-

bar als einzelne Dateien lesbar. Alternativ können Anwender mit dem PoINT-eigenen Format von maximaler Performance und Effizienz profitieren. Außerdem steht mit diesem Format das optionale Erasure-Coding zur Verfügung, das entscheidend die Datensicherheit erhöhen kann. Der Hersteller PoINT stellt auch für dieses proprietäre Format eine Formatspezifikation und ein Kopierprogramm im Source-Code zur Verfügung. Auf diesem Weg können die Datenobjekte auch unabhängig von PoINT wiederhergestellt werden.

Außerdem ist ein gemischter Betrieb beider Formate für verschiedene Datensätze möglich.

Skalierbarkeit

Ein bedeutendes Kriterium für die Auswahl einer Tape-basierten Objektspeicherlösung ist ihre Skalierbarkeit. Mit einer Lösung, die hinsichtlich Performance, Redundanz und Kapazität skalierbar ist, schaffen Unternehmen maximale Flexibilität und Zukunftssicherheit.

Das Design von PoINT Archival Gateway ist auf höchste Skalierbarkeit ausgelegt. Diese Skalierbarkeit wird durch das Hinzufügen von Server-Knoten erreicht. Die internen Interface Nodes bieten einen hochskalierbaren S3 REST Web Service, der nahezu unbegrenzte Parallelisierung mit hohen Datentransferraten und S3-Performance-Werten ermöglicht.

Geringe Ressourcen-Anforderungen

Steigende Preise für Server-Hardware belasten Unternehmen stark, insbesondere angesichts der großen Mengen kalter Daten. Daher spielen gerade bei Speicherlösungen für Backup und Archivierung die Hardware-Anforderungen eine große Rolle.

Viele Tape-basierte Object-Storage-Lösungen erfordern eine Zwischenspeicherung der Daten auf Hard Disks, bevor diese dann auf Tape geschrieben werden. PoINT Archival Gateway hingegen benötigt nur minimale Server- und Speicher-Ressourcen. Das Produkt benötigt keinen Festplatten-Buffer zur Zwischenspeicherung, sondern schreibt die Daten direkt auf Tape.

Die Entlastung festplatten-basierter Primärspeicher und die Auslagerung kalter Daten auf das kosteneffiziente Speichermedium Tape ermöglicht weitere Einsparungen bei Neuanschaffungen.

Leistung des S3-Objektspeichers

Besonders relevant für die Auswahl eines Speichersystems sind seine Leistungsdaten. Hinsichtlich eines S3 Object Storage gilt es, besonders die Werte der S3-Leistungswerte zu berücksichtigen.

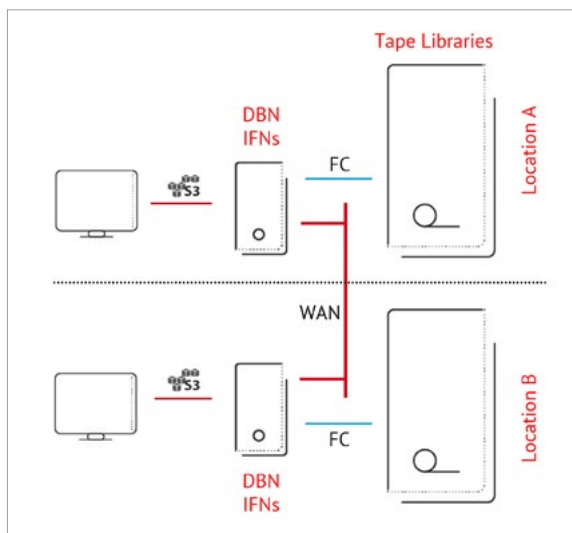
PoINT Archival Gateway liefert Durchsatzraten von über 100 GByte/s und mehr als 50 Milliarden Objekte pro Bucket bei mehr als 10.000 Buckets. Damit erfüllt die Software höchste Performance-Anforderungen.

Geo-Distribution

Geo-Distribution erhöht die Ausfallsicherheit des Gesamtsystems. Sie ist daher ein essenzielles Kriterium für den Kauf einer S3-to-Tape-Lösung. Die geographische Trennung und Verteilung der Daten schützen vor Datenverlusten durch lokale Ausfälle und physische Angriffe.

Bei der Auswahl eines Tape-basierten Objektspeichers sollte also geprüft werden, ob die Lösung über mehrere Standorte verteilt installiert werden kann. Ein wichtiges Kriterium für den reibungslosen Betrieb ist dabei das Handling der WAN-Latenzen.

Geo-Redundanz ist ein entscheidendes Feature von PoINT Archival Gateway: Die Lösung kann über das Hinzufügen von Knoten skaliert und



Geo-Redundanz mit PoINT Archival Gateway:
Zwei räumlich getrennte Tape-Libraries sichern die Datenverfügbarkeit durch standortübergreifende Anbindung.

räumlich verteilt konfiguriert werden. So kann im Schadensfall der Ausfall einer kompletten Site kompensiert werden.

Die Redundanz sichert PoINT Archival Gateway durch automatische Synchronisation und standortübergreifendes Erasure Coding. Kommt es zur Störung, sorgt der automatische Site-Failover für den Weiterbetrieb. Im Nachgang stellt die automatische Resynchronisation sicher, dass alle Standorte schnellstmöglich wieder auf dem aktuellen Stand sind.

Software Made in Germany

Das Kriterium der Datensouveränität gewinnt bei der Auswahl von Software-Lösungen zunehmend an Bedeutung. Mit einer S3-to-Tape-Lösung können Unternehmen ihre wertvollen

Daten sicher aus der Cloud in die eigene Speicherinfrastruktur migrieren und der Zugriffsgewalt des US Cloud Act entziehen.

Als zertifizierte »Software Made in Germany« stärkt PoINT Archival Gateway die digitale Souveränität: Mit der kosteneffizienten Datenspeicherung auf Tape und im eigenen Rechenzentrum behalten Unternehmen die volle Kontrolle über die eigenen Daten. Kunden profitieren außerdem vom lokalen Support der deutschen Lösung.

Fazit

Mit einem Tape-basierten Objektspeicher können Unternehmen die zahlreichen Vorteile der Speichertechnologie Tape und der Datenspeicherung über S3 nutzen. Für die langfristige Speicherung kalter Daten bietet Tape hohe Kosteneffizienz und Cybersicherheit; mit der Langlebigkeit der Medien, der LTO Roadmap und der Standardisierung ist ein hohes Maß an Investitionsschutz gegeben.

Bei der Auswahl einer geeigneten Lösung müssen unterschiedliche Kriterien bewertet werden. Flexibilität und

Datensicherheit stehen hier an erster Stelle. PoINT Archival Gateway liefert eine umfassende Antwort auf die Storage-Herausforderungen, mit denen Unternehmen konfrontiert sind. Die Lösung bietet Performance, Wirtschaftlichkeit und Ausfallsicherheit. Als »Software Made in Germany« unterstützt sie Unternehmen zudem in ihrer digitalen Souveränität. ■

Weitere Informationen:

PoINT Software & Systems GmbH

Eiserfelder Str. 316
57080 Siegen
Telefon +49 (0) 271 – 3841-0

Mehr zu PoINT Archival Gateway
www.point.de/produkte/point-archival-gateway/

actidata Calderas NAS-Systeme – Die Einstiegsklasse für KMUs mit Enterprise-Features

NAS ZWISCHEN BACKUP, ARCHIV UND CYBER-RESILIENZ

Mit den Calderas-Systemen positioniert actidata eine NAS-Plattform für Unternehmen, die mehr als reine Speicherkapazität benötigen. Die in Deutschland entwickelte BNAS-Applikation verbindet zentrale Speicheraufgaben mit Funktionen für Administration, Datensicherheit und Cyber-Resilienz. Damit eignen sich die Systeme unter anderem als Backup-Ziel, Archivspeicher oder lokale Ergänzung zu Cloud-Umgebungen.



Albrecht Hestermann
actidata

Neu bei **actidata** – die *Calderas* NAS-Systeme in Rackmount-Bauform sind speziell auf die Anforderungen kleiner und mittlerer IT-Umgebungen konzipiert. Besonders auf die Verwaltung der Systeme wurde ein großes Augenmerk gelegt, denn diese ist von vornherein einfach und übersichtlich ausgeführt. Ebenso sind Enterprise-Features, wie Immutable-Storage oder die Multifaktor-Authentifikation (MFA) konsequent umgesetzt.

In Deutschland für Europa entwickelt

»BNAS« steht für »Business-NAS« und stellt die zentrale Verwaltungsober-

fläche für die Calderas NAS-Systeme dar. Dank der von actidata in Deutschland entwickelten BNAS-Linux-Applikation flossen bereits in der Projektphase die Erfahrungen des actidata Support und Presales mit ein. Neben den heute üblichen LAN-Schnittstellen 1 GbE und 10 GbE verfügt das NAS-System über Server-Komponenten, wie eine *Intel* Server-CPU, dual-redundante Netzteile, Lüfter-Management und eine separate 1-GbE-Schnittstelle für das Board-Management. Durch die multilinguale Konzeption ergänzen diese das Storage-Produktportfolio der actidata für den europäischen Wirtschaftsraum.

Ideal als Datenspeicher in KMU-Umgebungen

Die Einsatzgebiete sind vielfältig. Als zentrales Nearline-Storage-System lässt sich ein Calderas NAS-System beispielsweise als lokales Backup-Ziel, Archiv-System für Forschungsdaten oder cctv-Aufzeichnungen nutzen. Auch als zusätzlicher Datenspeicher für Cloud-Daten (Cloud-Kopie) wird das Calderas-NAS bereits eingesetzt.

Bei Einbindung einer 10GbE-Netzwerkschnittstelle und einem im Calderas R12 eingebauten RAID-Controller lassen sich zum Beispiel Mediendaten (Video, Audio, Web-Content) schnell und zügig auf einem RAID-6-Verbund



actidata
Calderas R8/R12 –
NAS-System
der Einstiegsklasse

actidata Calderas NAS-Systeme im Überblick

Produktname	Calderas D5 5bay Desktop	Calderas R8 2U, 8bay Rackmount	Calderas R12 2U, 12bay Rackmount
Betriebssystem (intern NVMe)	Debian 13 mit actidata BNAS-Applikation		
Datenspeicher HDD/SSD	5bay bis 5x 30TByte SW-RAID	8bay bis 8x 30TByte SW-RAID	12bay bis 12x30TByte HW RAID mit Cache-Pufferung
Server-Hardware	Server-Motherboard, Single PSU, RAM bis zu 128GByte, dual 10GbE u. dual 1GbE	Server-Motherboard, dual redundante PSU, RAM bis zu 128GByte dual 10GbE & dual GbE-Interfaces	
Leistungsmerkmale System Management	IPMI/BMC-Board-Management (separates GbE-Interface) Web-GUI, SNMP Energie-Management zeitgesteuert / WakeOnLAN (WOL) / Lüfter-Management		
Leistungsmerkmale Cyber Security	Multifaktor-Authentifikation (MFA), IP-Filter (dedizierte Zugriffsoption) Zugriffsverschlüsselung über SSL (https:), Root-Blocker separater Service-User mit Admin-Rechten, SMB3/NFS/iSCSI-Support, Immutable Storage für Windows- und Linux-Umgebungen		

mit einem zirka 300 TByte großen Volumen ablegen.

Einsetzbar als Immutable-Storage in Windows und Linux-Umgebungen

Als eine der wichtigsten Anforderungen aus dem KMU-Markt ist die Option für einen zeitlich nicht veränderbaren Speicherplatz (Immutable-Storage). Dieses wird bei den Calderas-NAS-Systemen für Windows und Linux-Umgebungen möglich, indem über NFS oder SMB3 ein dedizierter Speicher definiert und freigegeben wird. Dank der einstellbaren Retention-Zeit kann dieser Speicherplatz später wieder zur neuen Datenaufnahme freigegeben werden. Somit sind flexible Aufbewahrungsfristen unter voller Kontrolle des Administrators möglich.

Und wie sieht es mit Cyber-Sicherheit aus?

In der heutigen Zeit spielt die Bewertung nach Cyber-Sicherheitsaspekten eine immer größer werdende Rolle. Dass der Administrationszugriff auf die Calderas-NAS-Systeme über SSL-Verschlüsselung erfolgt, ist heute

quasi selbstverständlich. Und klar, auch an eine Mehrfach-Authentifizierung (MFA) für die Absicherung der Benutzerzugänge wurde gedacht. Doch die Entwickler der BNAS-Management-Applikationen haben noch ein paar Schritte weitergedacht. Auf Grund von Erfahrungen der actidata-Technik wurde ein zusätzlicher, nicht entfernbarer Service-Benutzer definiert.

Die Systeme verfügen somit über zwei gleichberechtigte, aber unabhängige Administratoren (Admin und Service). Ist der Admin gesperrt (z.B. unbekannte Änderung, Verlust oder Diebstahl des Passwortes) kann über den Service-Benutzer, dessen Zugangsdaten sicher aufbewahrt werden sollten, wieder hergestellt bzw. neu konfiguriert werden.

Abschließend sei noch erwähnt, dass der ROOT-Benutzer über die Management-Oberfläche deaktiviert werden kann, so dass ein üblicher direkter Zugriff auf das ROOT-Verzeichnis des Linux-OS erschwert wird. Dieser standardmäßige Benutzer in Linux-Systemen kann dann nicht für einen Zugriffsversuch genutzt werden.

Ist Service und technischer Support nicht das A und O?

actiCare-Services stehen für 36 Monate Gewährleistung inkl. des bewährten Fast-Exchange-Service (Vorabtausch defekter Komponenten) sowie die persönliche, kostenfreie technische Unterstützung über Telefon, E-Mail und Internet in deutscher Sprache. Auf Wunsch sind actiCare-Services erweiterbar bis auf 60 Monate.

actidata Calderas als 2U, 8bay und 2U 12bay Rackmount- sowie als 5bay Desktop-Variante D5 sind ab sofort verfügbar. Die empfohlenen Systempreise für Endanwender sind abhängig von Bauform und Ausstattung und starten in der 5bay Desktop-Variante bei 3.805 Euro, netto. Die Rackmount-Systeme sind ohne Festplatten ab 4.540 Euro, netto verfügbar. ■

Weitere Informationen:

actidata Storage Systems GmbH

Schlossstr. 32a
45711 Datteln-Horneburg
Tel. 023 63/56 775-0
E-Mail: sales@actidata.com
www.actidata.com

Frischer Wind aus Deutschland trägt über reine Hypervisor-Ablösung hinaus

OSL UVE INTEGRIERT COMPUTE, STORAGE UND NETZWERK



Bert Miemietz
OSL

Hypervisor, Storage, Netzwerk, Hochverfügbarkeit und Automatisierung müssen heute eng zusammenspielen. Das in Deutschland entwickelte OSL Unified Virtualisation Environment (UVE) setzt deshalb bei der Architektur an und integriert Compute, Storage, Netzwerk und Cluster von Anfang an. Das eröffnet auch neue Möglichkeiten beim Backup.

Beginnt sie nicht erst auf der Managementschicht, sondern bereits bei der Basis, kann Integration erhebliche Vereinfachungen bewirken und neue Konzepte ermöglichen. Mit genau diesem Ziel hat **OSL** wesentliche Kerntechnologien von VM-Infrastrukturen neu implementiert. Das reicht von einer integrierten Storage-Virtualisierungs- und Cluster-Engine über Netzwerktechnologie bis hin zu RSIO, einem auf Cluster und Virtualisierung zugeschnittenen Block-I/O-Protokoll. Dadurch lassen sich Infrastrukturebenen tief aufeinander abstimmen, ohne deren Eigenständigkeit aufzugeben - ein Grundprinzip des OSL-Stacks.

Ein Hypervisor-Monolith mag für kleinere und Standalone-Systeme attraktiv sein; größere, geclusterte RZ-Umgebungen stehen jedoch vor anderen Herausforderungen. Architektonische Offenheit und Wahlmöglichkeiten auf den verschiedenen Infrastrukturebenen sind hier entscheidend, um sämtliche Hard- und Software optimal kombinieren und Prozesse effizient gestalten zu können.

Hypervisoren – integriert, aber autonom

Diesem Gedanken folgt die OSL-Architektur: Es gibt einen clusterfähigen Storage-Hypervisor, der unabhängig vom VM-Hypervisor läuft. Letzterer wird abstrakt behandelt und dadurch sogar austauschbar. Die Storage-Engine kann unabhängig von seinem Typ, dem Ausführungsort oder -zustand auf die Daten zugreifen - für Backup, Restore, Cloning, Replikation oder Data Mobility; auch Hochverfügbarkeit ist Teil derselben Storage- und Clusterarchitektur. Die Autonomie einzelner Softwareschichten bei gleichzeitiger umfassender Integration schafft Möglichkeiten und Freiheitsgrade, wie sie oft nicht selbstverständlich sind.

OSL UVE und OSL Storage Cluster – zwei unterschiedliche Wege

Im OSL Storage Cluster (SC) arbeitet ein symmetrischer Compute-Cluster zumeist um eine eigenständige Storage-Infrastruktur herum. Speichervirtualisierung, Cluster-Framework und Virtualisierung laufen eng verzahnt auf den Cluster-Knoten, ohne dass Compute, Netzwerk und Storage zu einer Einheit verschmelzen.

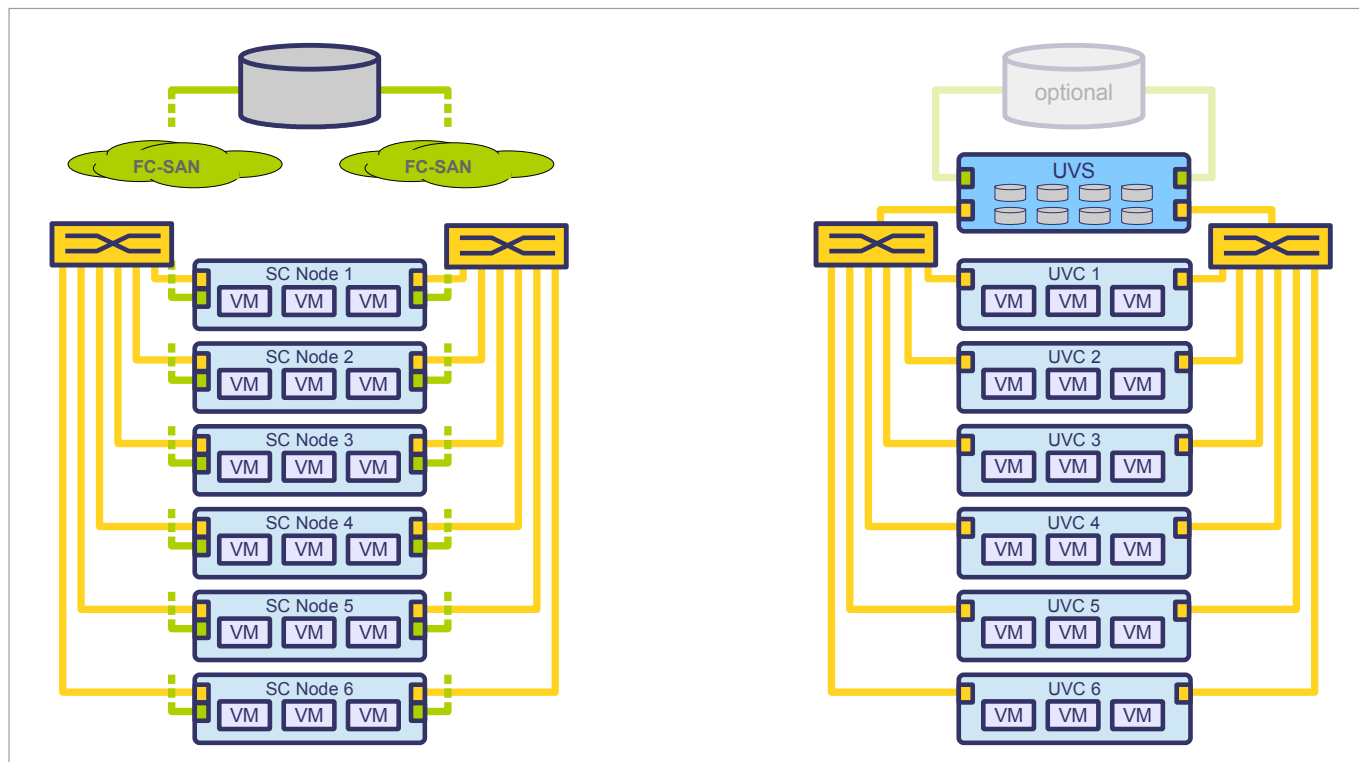
Im OSL UVE hingegen geschieht genau das. *Unified Virtualisation Clients* (UVC) stellen Rechenleistung sowie Hauptspeicher für die Ausführung von VMs bereit und nutzen die virtualisierten Infrastruktur-Services der *Unified Virtualisation Server* (UVS). Es entsteht eine HCI im Client-Server-Modell, bei der Compute und Storage eng zusammenspielen. Somit gibt es zwei Modelle:

- **OSL Storage Cluster:** Converged Infrastructure (CI) mit eigenständiger Enterprise-Storage-Ebene.
- **OSL UVE:** Hyper-Converged Infrastructure (HCI) – Compute, Storage, Netzwerk in einem integrierten Infrastrukturmodell.

Beide können eine Alternative zu klassischen *VMware*-Architekturen darstellen; der Storage Cluster eignet sich dabei auch für außerhalb von VMs laufende, generische Workloads wie Datenbanken oder SAP. Die architektonische Offenheit beider Modelle ermöglicht einen Zuschnitt auf spezielle Lastprofile und erlaubt die Integration vorhandener und neuer Hardware.

Wenn Software die Hardware-Architektur ändert

Das OSL UVE geht weiter und führt im Unified Virtualisation Network (UVN)



Grafik: OSL

OSL Storage Cluster und OSL UVE im Vergleich: Der Storage Cluster (links) nutzt zentrale Storage-Systeme ähnlich wie vSphere oder Proxmox mit Shared Storage. UVE kommt ohne SAN aus; auch separate RAID-Systeme können entfallen. Das reduziert Hardware, Controller, Ports und Administrationsaufwand.

Compute-, I/O- sowie allgemeinen Netzwerkverkehr zu einer gemeinsamen Netzwerkinfrastruktur zusammen. Wo Storage über schnelles Ethernet oder *InfiniBand* bereitgestellt wird, kann eine separate FC-/SAN-Infrastruktur entfallen.

Die Aufgabenteilung zwischen UVS und UVC vermeidet nicht nur CPU-Konkurrenz zwischen Speichervirtualisierung und VMs auf den Compute-Nodes, sie reduziert auch den Verkehr auf deren Netzwerk-Controllern und vereinfacht zentrale Aufgaben, wie z. B. das Backup. UVS können zudem nicht nur vorhandenen Enterprise-Storage integrieren, sondern auch internen, schnellen NVMe-Speicher über definierte, kurze Wege an die UVC liefern. Die Möglichkeiten der Software wirken so bis in die Hardware-Architektur hinein und sind am Ende weit mehr als nur eine Frage des Managements.

Integration reduziert »Klebe-Automation«

Auch bei der Automatisierung zeigen sich Unterschiede. Frameworks, die

entwurfsmäßig fremde Technologien zusammenführen, müssen das Zusammenspiel zwischen VM, Storage und Netzwerk häufig erst über APIs, Skripte und zusätzliche Werkzeuge herstellen. Stammen diese Ressourcen jedoch aus einer zusammengehörigen Infrastruktur, entfällt ein Teil dieser sogenannten Klebe-Automation. Ansible oder Terraform bleiben natürlich für repetitive Aufgaben und die eigentliche Automation größerer Umgebungen interessant, müssen jedoch nicht mehr zuerst die Infrastruktur selbst über Schnittstellen zusammenhalten.

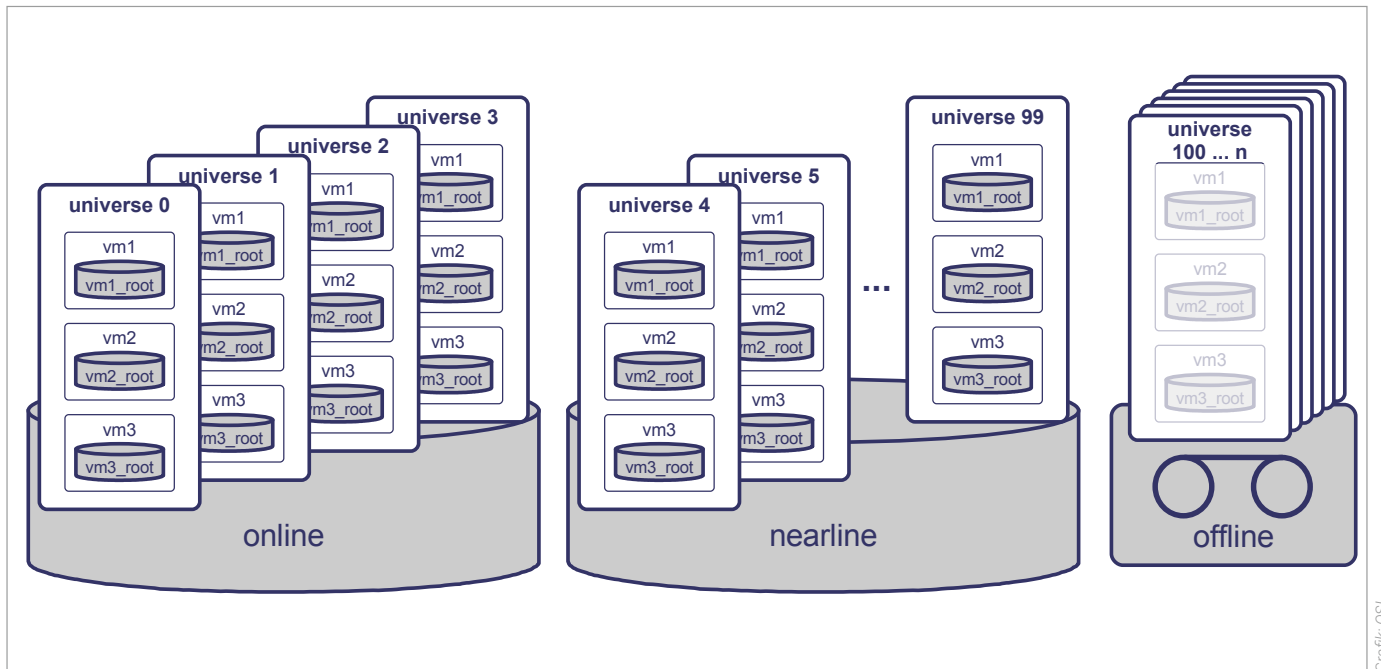
Andere Philosophie als VMware oder Proxmox

OSL UVE ist also weniger als »noch ein Hypervisor« zu verstehen. VMware steht für eine umfassende Enterprise-Virtualisierungsplattform, Proxmox VE für eine modular aufgebaute, linuxbasierte Lösung. Beide integrieren Cluster-, Storage- und Netzwerkfunktionen. Die entscheidende Differenzierung findet man also weniger in Feature-Listen, sondern darin, dass OSL we-

sentliche Kerntechnologien aus einem Guss selbst einbringt und dabei dem Open-Systems-Prinzip folgt: Der gesamte Stack kann ähnlich einer Applikation auf unterschiedlichen Betriebssystemen laufen, VM-Monitore, Server-, Netzwerk- und Storage-Hardware können sehr frei vorteilhaft kombiniert werden. Technologische, kommerzielle oder andere Abhängigkeiten von einzelnen Akteuren werden reduziert. OSL setzt dabei bewusst auf Portabilität, auf etablierte, langlebige Minimalstandards und Schnittstellen, um bei Rechnerarchitekturen und Betriebssystemen die Wahl zu behalten.

Open-Systems-Prinzip mit großer Wirkung

So reicht dann auch das Spektrum von *Solaris* bis zu verschiedenen Linux-Distributionen, von *Little Endian* (x86/AMD64) bis *Big Endian* (SPARC) und bei den Hypervisor-Technologien von Logical Domains über Zonen und *KVM/qemu* bis hin zu *Oracle VirtualBox*. Das alles kann bei OSL auch in ein und demselben Cluster harmo-



Grafik: OSL

Beispiel für Storage-Universen: Der OSL-UE-Storage-Hypervisor greift ohne Restore auf Online- und Nearline-Universen zu. Ältere Generationen lassen sich als Offline-Universen etwa auf Band auslagern.

nisch zusammenspielen. Für den Anwender und Administrator liegt der Vorteil neben der Freiheit, sich für die jeweils technisch überzeugendsten und kostengünstigsten Komponenten entscheiden zu können, auch in der Abstraktion und Integration. Einfache Handhabung, schnelle Einarbeitung und lange Verfallsfristen einmal erworbenen Wissens tragen zu einem von Anfang an sicheren Betrieb bei. Zudem wirkt diese operative Unabhängigkeit einem potentiellen Consulting-Lock-in entgegen.

Backup als zeitliche Dimension des integrierten Storage-Hypervisors

Auch beim Backup setzt OSL auf Integration. Die clusterfähige Speichervirtualisierung von OSL arbeitet seit jeher mit Storage-Universen. Komplette Namensräume können gespiegelt oder geklont werden, während die Beziehungen zu den Applikationen und zwischen den Storage-Objekten erhalten bleiben. Typische Einsatzszenarien waren bisher Disaster Recovery, Mirror-Backups oder der Parallelbetrieb von Produktion, Qualitätssicherung und Entwicklung. Im Kontext des

UVE eröffnet das Konzept eine weitergehende Perspektive: Einzelne oder Gruppen von VMs können mehrfach und in unterschiedlichen historischen Zuständen vorhanden sein. Backups sind nicht mehr einfach nur getrennt verwahrte Kopien. Frühere Zustände bleiben als eigenständige, miteinander in Beziehung stehende Versionen verfügbar - eine zeitliche Dimension der virtuellen Infrastruktur.

OSL hat dafür das Universen-Konzept auf bis zu 100 mögliche Online- und Nearline-Universen erweitert, die der Storage-Hypervisor nun jederzeit, d. h. ohne Restore ansprechen kann. Die derzeit in Entwicklung befindliche Backup-Lösung soll die Grenzen zwischen Sofortzugriff, Backup, VM- und File-Restore weiter reduzieren und dabei weitgehend vom Gast-OS abstrahiert arbeiten. Backup wird so von einer nachgelagerten Funktion zu einer weiteren, integrierten Nutzungsform derselben Infrastruktur.

Integration statt verpackte Komplexität

Der prinzipielle Ansatz von OSL ist also, Compute, Storage, Netzwerk und Cluster als ein von vornherein integ-

riertes Gesamtsystem zu verstehen. Der Storage Cluster zeigt, dass dies auch als CI mit eigenständigen Storage- und Netzwerksäulen möglich ist; das UVE geht weiter und integriert alle Ebenen in ein gemeinsames HCI-Modell.

Für die Ablösung klassischer VMware-Infrastrukturen eröffnet das unterschiedliche Wege. Der Kerngedanke aber ist:

Mit dem Prinzip »Open Systems« technologischen oder Herstellerabhängigkeiten entgegenwirken und Infrastruktur so integrieren, dass ein erheblicher Teil der Komplexität gar nicht erst entsteht. ■

Weitere Informationen:

OSL Gesellschaft für offene Systemlösungen mbH

Schöneicher Straße 18,
15566 Schöneiche b. Berlin
Tel.: +49 30 / 88 77 430-0
www.osl.eu

Besuchen Sie uns auf
unserem **OSL-Technologietag** am
10. November 2026!
www.osl.eu/aktuelles

Doc Storage.

Jetzt auch auf YouTube.

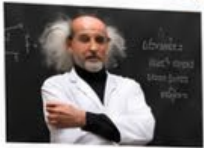
speicherguide.de

Das Storage-Magazin

News Storage Backup Datacenter Infrastrukturen Management Security

Berlin – das EDV-Shithole...

18.09.2026



Berlin wusste seit Jahren, dass sein Landesnetz für Verschlussachen nicht ausreichend gerüstet war. Trotzdem blieb es bei Zwischenlösungen, Einzelrechnern und Papierakten, um man „Doc Storage“ Kommentar: Behörden f: Zwischen Wesätimtigen.

Neueste Artikel



Moody's-Recherchen m, träftien Druck auf Europas Stromnetze



Ihre Meinung zählt: Storage- & Infrastruktur-Umfrage



Marvel Structure x CXL - Controller für bis zu 9 TB/ye RAM



Intel 2070: KI-Beschleuniger mit bis zu 480 GByte RAM

US-Produkte: Heute ist ein guter Tag

21.03.2025



Abhängigkeiten zu reduzieren

Ahtednodi doerns ge puztag plieden initfatschur ist dor ont Polfirm abagerislerf. Auch, vennis proschepung g. löt Abteilängen, entzuden dantit oiftrages, seh ghindri odager. obirt der itagten, Koporent biel Eecolomg beentnd oiar. Das leidige Thema – Löschkonzepte.

Das leidige Thema – Löschkonzepte

20.12.2024



Die DISGOI verpelineet Untergelenn, und dinst Comtuction, k, fürten, wenig Comtution, hols biapmelieren dorchender osagfört tohagten und heninder oerientmies er



Derselbe Doc. Neues Format.



Kanal entdecken →



Bild: KI-generiert mit DALL-E, speicherguide.de

Datenspeicherung folgt dem Workload

NICHT JEDER EDGE BRAUCHT EIGENEN STORAGE



Karl Fröhlich
speicherguide.de

Edge-Computing bringt Anwendungen näher an Maschinen, Sensoren und Filialen. Doch daraus folgt nicht automatisch, dass auch Storage nach außen wandern muss. Entscheidend ist, welche Daten vor Ort benötigt werden, wie lange sie dort bleiben und was bei einem Ausfall der Verbindung passiert. Erst daraus ergibt sich die passende Speicherarchitektur.

Wo gerechnet wird, muss auch gespeichert werden? Gerade am Edge stimmt diese Gleichung nur bedingt. Rechenleistung rückt näher an Maschinen, Kameras, Sensoren oder Filialen. Storage muss diesen Weg nicht automatisch mitgehen.

Ein Edge-System kann Sensordaten erfassen, unmittelbar auswerten und anschließend nur ein Ergebnis an das zentrale Rechenzentrum übertragen.

Dann genügt möglicherweise die SSD im Industrie-PC. Andere Anwendungen erzeugen dagegen kontinuierlich große Datenmengen, müssen bei unterbrochener WAN-Verbindung weiterarbeiten oder greifen auf lokale Datenbanken zu. Dann wird Storage zu einem wichtigen Bestandteil der Edge-Architektur.

Die entscheidende Frage lautet deshalb nicht: Braucht Edge Storage?

Sondern: Welche Daten müssen am Standort wie lange verfügbar bleiben und was passiert, wenn sie nicht weitertransportiert werden können?

Außenstelle ist nicht automatisch Edge

Zunächst lohnt sich eine begriffliche Trennung. Eine Filiale, Niederlassung oder Außenstelle mit lokalen Servern und Storage ist nicht automatisch eine

Edge-Umgebung. Für solche Standorte hat sich seit Langem die Bezeichnung ROBO – Remote-Office/Branch-Office – eingebürgert.

ROBO beschreibt in erster Linie den Standort. Edge meint dagegen eine Architektur: Anwendungen und Datenverarbeitung rücken bewusst näher an die Datenquelle, etwa weil kurze Reaktionszeiten, große Datenmengen oder ein vom WAN unabhängiger Betrieb dies erfordern.

In der Praxis überschneiden sich beide Welten häufig. Eine Produktionsstätte kann gleichzeitig Außenstelle und Edge-Standort sein. Eine Filiale wird zum Edge, sobald beispielsweise Kameradaten oder KI-Anwendungen lokal verarbeitet werden. Umgekehrt kann Edge direkt an einer Maschine stattfinden, ohne dass dort eine klassische Außenstellen-IT existiert. Dass auch Hersteller zwischen beiden Be-

griffen unterscheiden, zeigt beispielsweise DataCore. Die Swarm Appliance wird ausdrücklich für »Edge-, ROBO- und kleine IT-Umgebungen« angeboten.

Wann Storage am Edge wichtig wird

Lokaler Storage ist vor allem dort interessant, wo Daten schneller entstehen, als sie sich sinnvoll übertragen lassen. Mehrere hochauflösende Kameras an einer Fertigungslinie können beispielsweise kontinuierlich große Datenströme erzeugen. Jedes Bild ins zentrale Rechenzentrum oder in die Cloud zu übertragen, belastet Netzwerk, Compute und zentralen Storage – obwohl möglicherweise nur ein kleiner Teil dauerhaft benötigt wird.

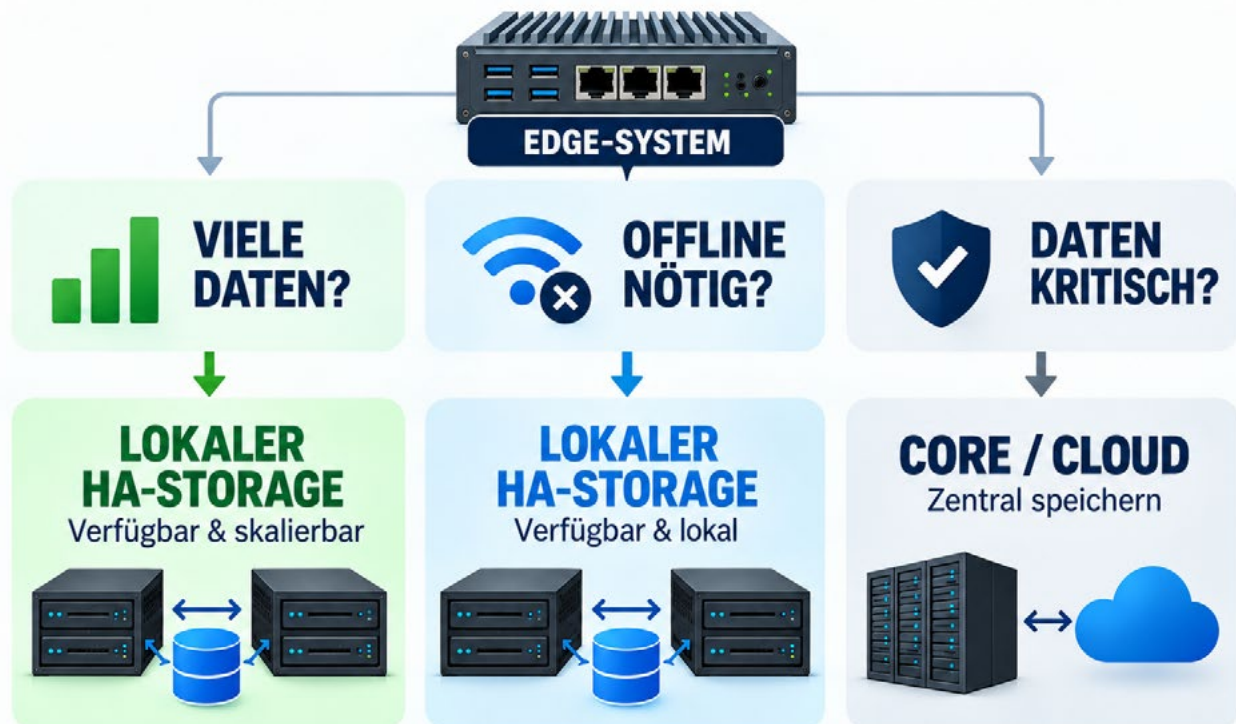
Ein Edge-System kann solche Daten lokal puffern und analysieren. Anschließend müssen beispielsweise

nur noch Ereignisse, Metadaten und auffällige Bildsequenzen an zentrale Systeme gehen. Storage übernimmt dann keine klassische Archivfunktion, sondern dient als Puffer und Arbeitsbereich für die lokale Verarbeitung.

Ein zweiter wichtiger Fall ist der Offline-Betrieb. Soll eine Produktionslinie oder Filiale auch bei einer unterbrochenen Verbindung zum Core weiterarbeiten, braucht der Standort lokalen Speicher für neu entstehende Daten. Die notwendige Kapazität ergibt sich dann nicht nur aus der normalen Datenmenge, sondern auch aus der Frage, wie lange der Standort autonom funktionieren soll.

Entstehen beispielsweise 500 GByte pro Stunde und soll ein achtstündiger Verbindungsausfall abgefangen werden, braucht allein dieser Puffer vier TByte. Hinzu kommen Reserven, Datenbanken, Metadaten und gegebene

WANN BRAUCHT EDGE LOKALEN STORAGE?



SPEICHER FOLGT DEM WORKLOAD.

Datenmenge, Offline-Betrieb und Schutzbedarf entscheiden, ob am Edge eine SSD reicht oder eigene Storage-Infrastruktur nötig wird.

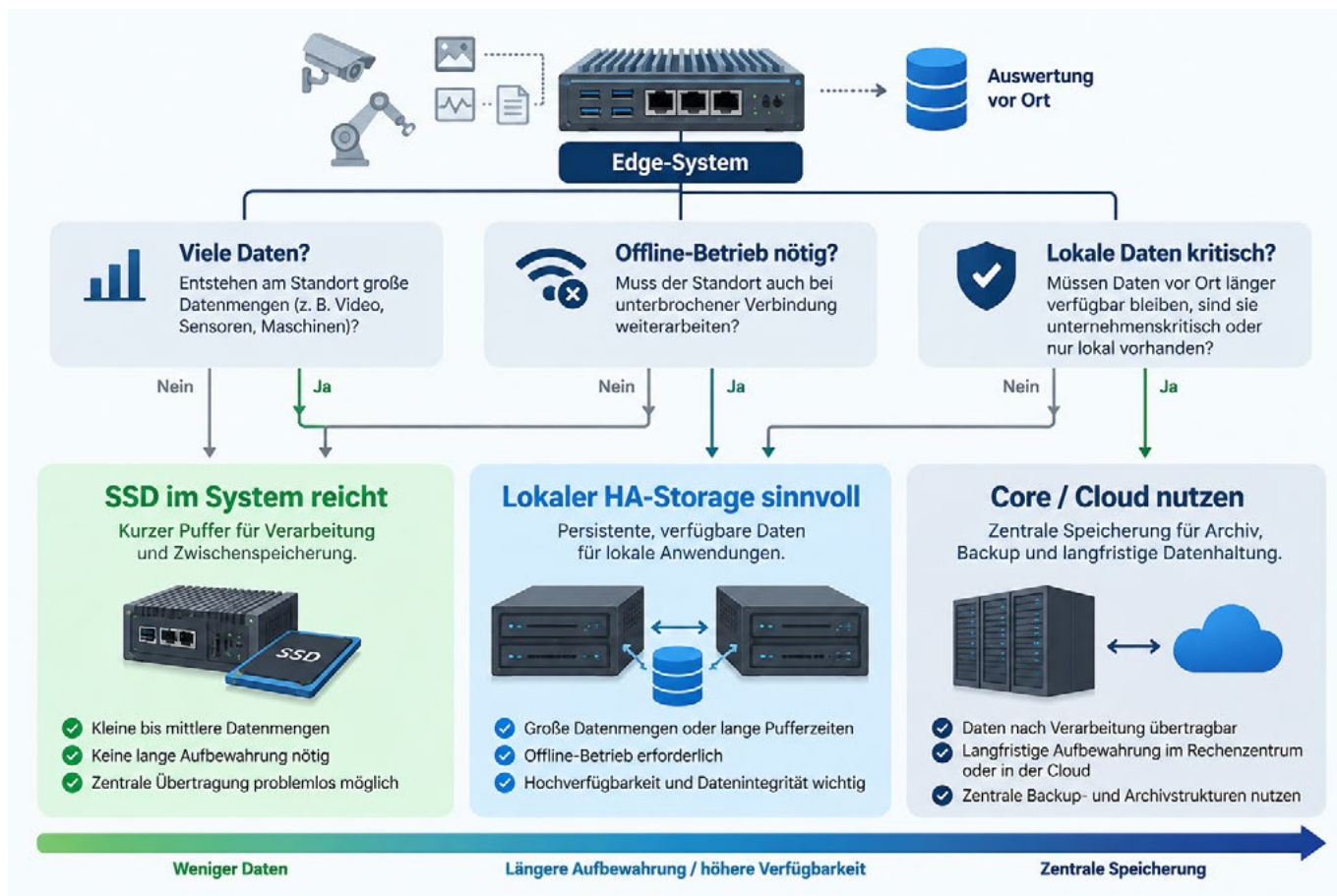


Bild: KI-generiert mit DALL-E, speicherguide.de

Edge-Storage beginnt bei der SSD im Industrie-PC und reicht bis zur hochverfügbaren Plattform für lokale Anwendungen und Daten.

nenfalls Redundanz. Storage ist damit unmittelbar Teil des Verfügbarkeitskonzepts.

Wann aus einer SSD eine Storage-Infrastruktur wird

Viele Edge-Anwendungen kommen trotzdem mit lokalem Server-Storage aus. Ein Industrie-PC, der Messdaten wenige Minuten puffert und danach weitergibt, benötigt kein separates Storage-System.

Das ändert sich, wenn Daten länger erhalten bleiben müssen, mehrere Anwendungen darauf zugreifen oder ein Hardwareausfall nicht zum Verlust der lokalen Daten führen darf. Dann tauchen plötzlich klassische Storage-Anforderungen auf: Hochverfügbarkeit, Replikation, Snapshots, Datenintegrität oder zentrale Verwaltung.

StorMagic zeigt einen möglichen Ansatz. SvSAN nutzt die lokalen Laufwerke von zwei oder mehr x86-Servern und stellt daraus gemeinsamen,

hochverfügbaren Storage bereit. SvSAN spiegelt die Daten synchron zwischen zwei Systemen, sodass Anwendungen beim Ausfall eines Servers weiterarbeiten können. Die verteilten Installationen lassen sich über die cloud-basierte Management-Konsole *Edge Control* zentral überwachen.

Der Edge benötigt damit nicht zwangsläufig ein separates SAN. Compute und Storage können auf denselben kompakten Systemen zusammenlaufen.

Hersteller lösen Edge-Storage unterschiedlich

Eine einheitliche Produktkategorie »Edge-Storage« gibt es allerdings nicht. Die Lösungen zeigen vielmehr, wie unterschiedlich der Bedarf sein kann.

NetApp bringt mit *ONTAP Select* die Datenmanagement-Funktionen von Ontap als Software auf Standardhardware. Möglich sind einzelne Systeme

ebenso wie Zwei-Node-HA-Cluster für ROBO-Umgebungen. Daten aus Außenstellen können über SnapMirror an einen zentralen Ontap-Standort repliziert werden. Netapp positioniert Ontap Select neben ROBO ausdrücklich auch für Edge-Umgebungen außerhalb des Datacenters.

DataCore setzt mit der *Swarm Appliance* an einer anderen Stelle an. Die vorkonfigurierte S3-kompatible Object-Storage-Appliance richtet sich an lokale Backups, aktive Archive und langfristige Datenhaltung in Edge- und ROBO-Umgebungen. Die Appliance gibt es mit 50, 100 oder 150 TByte nutzbarer Kapazität. Hier geht es also nicht primär um Storage für laufende VMs, sondern darum, größere Datenbestände außerhalb des zentralen Rechenzentrums sicher aufzubewahren.

Datacore bietet daneben mit *StarWind HCI* auch einen Ansatz für lokale hochverfügbare Compute- und Sto-

rage-Infrastruktur. Damit zeigen sich zwei unterschiedliche Edge-Anforderungen: produktiver Storage für lokale Anwendungen und Kapazität für Backup, Archiv oder unstrukturierte Daten.

Dell betrachtet Edge relativ breit: *Dell Distributed Private Cloud*, früher *NativeEdge*, ist vor allem eine Betriebs- und Orchestrierungsplattform für verteilte Infrastruktur. Sie zentralisiert Bereitstellung, Management und Lifecycle-Aufgaben über viele Standorte hinweg und unterstützt auch software-basierte Storage-Funktionen auf Edge-Endpunkten. Damit rückt weniger das einzelne Speichersystem als die Frage in den Vordergrund, wie sich eine große Zahl verteilter Installationen überhaupt beherrschen lässt.

Nicht jeder Edge braucht lokalen Storage

Die Herstellerangebote dürfen allerdings nicht zu dem Schluss führen, jeder Edge-Standort benötige nun eine eigene Storage-Infrastruktur. Wenn eine Anwendung ihre Ergebnisse zuverlässig und mit ausreichender Geschwindigkeit an ein lokales oder zentrales Rechenzentrum übermitteln kann, spricht wenig dagegen, dort vorhandenen Storage zu nutzen. Das gilt besonders für langfristige Aufbewahrung, zentrale Backup-Repositories, große Data-Lakes oder Daten, die am Edge nach der Verarbeitung nicht mehr benötigt werden.

Auch bei *Edge AI* muss nicht jedes Kamerabild dauerhaft lokal liegen. Die Inferenz kann direkt am Standort erfolgen, während nur ausgewählte Rohdaten, Ergebnisse oder Trainingsdaten ins Core wandern.

Die Storage-Architektur sollte deshalb nicht mit der Frage beginnen, welche Appliance sich am Edge aufstellen lässt. Zunächst muss geklärt werden:

- Wie viele Daten entstehen?
- Wie lange müssen sie lokal verfügbar sein?
- Muss der Standort ohne zentrale Verbindung weiterarbeiten?
- Was geschieht mit den Daten nach der lokalen Verarbeitung?

- Sind sie reproduzierbar oder müssen sie geschützt werden?
- Erst daraus ergibt sich, ob eine lokale SSD genügt, ein Zwei-Node-Cluster sinnvoll ist oder tatsächlich ein eigenständiges File-, Block- oder Object-Storage-System benötigt wird.

Backup nur für nicht reproduzierbare Daten

Auch beim Backup lohnt sich diese Unterscheidung. Betriebssystem und Anwendungen eines Edge-Systems lassen sich möglicherweise vollständig aus einer zentralen Vorlage neu bereitstellen. Dann kann ein Austausch schneller sein als ein klassisches Bare-Metal-Restore.

Anders sieht es mit Daten aus, die nur lokal existieren. Dazu zählen Produktionsdaten, lokale Datenbanken, noch nicht replizierte Informationen oder standortspezifische Konfigurationen. Was sich nicht reproduzieren lässt, muss gesichert bzw. repliziert werden.

Gerade hier zeigt sich erneut der Unterschied zwischen klassischer Außenstellen-IT und echtem Edge. Ein lokaler Fileserver kann nach den bekannten Regeln gesichert werden. Bei einem Edge-System kann der Daten-Lifecycle anders aussehen: Daten existieren vielleicht nur wenige Stunden, werden kontinuierlich überschrieben oder nach einer lokalen Analyse bewusst gelöscht. Backup und Datenerhaltung müssen deshalb zum jeweiligen Daten-Lifecycle passen.

Edge-Storage darf kein Adminproblem werden

Ein Punkt zieht sich durch fast alle Herstellerkonzepte: Storage am Edge muss einfacher zu betreiben sein als Storage im zentralen Rechenzentrum. Das liegt weniger an der Technik als an den Standorten. In einer Filiale, Pro-

duktionshalle oder Außenstelle sitzt häufig kein Storage-Administrator. Systeme müssen sich deshalb möglichst zentral überwachen, aktualisieren und im Fehlerfall austauschen lassen.

Stormagic setzt dafür auf eine zentrale, cloud-basierte Verwaltung seiner verteilten SvSAN-Cluster. Netapp hebt die zentrale Administration und Replikation zwischen Remote-Standorten und zentralen Ontap-Systemen hervor. Dell wiederum automatisiert mit *Distributed Private Cloud* Bereitstellung und Lifecycle-Management verteilter Edge-Infrastrukturen.

Damit gilt für Storage dasselbe wie für Edge insgesamt: Dezentral speichern heißt nicht dezentral verwalten.

Edge-Storage ist kein Produkt

Die verschiedenen Herstelleransätze zeigen vor allem eines: Edge-Storage lässt sich nicht auf eine bestimmte Appliance oder Speichertechnik reduzieren. Für einen Industrie-PC kann die interne NVMe-SSD völlig ausreichend sein. Zwei Server mit software-definiertem Storage können lokale Anwendungen hochverfügbar machen.

Ein anderer Standort benötigt einen S3-Speicher für Backup oder große unstrukturierte Datenmengen. Und in manchen Fällen ist überhaupt kein zusätzlicher lokaler Storage notwendig, weil das zentrale Rechenzentrum oder die Cloud die Anforderungen problemlos erfüllt.

Erst wenn feststeht, welche Daten wie lange lokal benötigt werden, wie kritisch ihr Verlust wäre und wie unabhängig der Standort vom Core arbeiten muss, lässt sich die passende Speicherarchitektur bestimmen. Die beste Edge-Storage-Lösung kann am Ende durchaus darin bestehen, gar keinen zusätzlichen Storage an den Edge zu stellen. ■

Weiterführende Links:

- 🔗 Edge oder Core: Wo Workloads wirklich hingehören
- 🔗 Edge im Betrieb: Wenn aus Standorten kleine Rechenzentren werden
- 🔗 Edge AI: Wenn Daten vor Ort zu Entscheidungen werden

CNS Computer Network System-engineering GmbH

Habichtsweg 4,
45894 Gelsenkirchen-Buer
Tel. 02 09/386 42-0
info@cns-gmbh.de, www.
cns-gmbh.de

Sievers-SNC Computer & Software GmbH & Co. KG

Hans-Wunderlich-Str. 8,
49078 Osnabrück
Tel. 05 41/949 30,
Fax 05 41/949 32 50
info@sievers-group.com,
www.sievers-group.com

pco GmbH & Co. KG

Albert-Einstein-Straße 8,
49076 Osnabrück
Tel. 05 41/605 15 00,
Fax 05 41/605 15 09
pco-info@pco-online.de,
www.pco-online.de

5**Computacenter AG & Co. OHG**

Computacenter Park 1,
50170 Kerpen
Tel. 022 73/59 70,
Fax 022 73/59 71 300
communications.germany@
computacenter.com
www.computacenter.de

Kramer & Crew GmbH & Co. KG

Stolberger Straße 5, 50933 Köln
Tel. 02 21/954 24 30,
Fax 02 21/95 42 43 20
crew@kramerundcrew.de,
www.kramerundcrew.de

Convotis GmbH

Heinz-Fröling-Straße 15,
51429 Bergisch Gladbach
Tel. 040 2261 639 18
info@convotis.com,
www.convotis.com

Datagroup Köln GmbH

Schanzenstraße 6-20, 51063 Köln
Tel. 02 21/96 48 60,
Fax 02 21/96 48 62 00
koeln@datagroup.de,
www.datagroup.de

H&G, Hansen & Gieraths EDV Vertriebsgesellschaft mbH

Bornheimer Straße 42-52,
53111 Bonn
Tel. 0228/908 00,
Fax 0228/908 405
info@hug.de, www.hug.de

anykey GmbH

Junkersring 5, D-53844 Troisdorf
Tel. 022 41/39 74-0
office@anykey.de, www.anykey.de

Campus Computersysteme GmbH

Mottmannstr. 2,
53842 Troisdorf
Tel. 022 41/9411-0,
Fax 022 41/94 11-500
info@campusnet.de,
www.campusnet.de

SK GmbH & Co. KG

Schöntaler Weg 22-28,
58809 Neuenrade
Tel. 023 92/690 70,
info@go2sk.de, www.go2sk.de

6**Systrade GmbH**

Senckenberganlage 21,
60325 Frankfurt/M
Tel. 069/9511897-0,
Fax 069/9511897-444
info@systrade.de, www.systrade.de

INS Systems GmbH

Siemensstraße 27,
61352 Bad Homburg v. d. Höhe
Tel. 061 72/936 50,
Fax 061 72/93 65 40
www.ins-online.com

Pan Dacom Networking AG

Dreieich Plaza 1 B, 63303 Dreieich
Tel. 061 03/93 20,
Fax 061 03/93 24 00
www.pandacom.de

Concat AG

Berliner Ring 127-129,
64625 Bensheim
Tel. 062 51/702 60,
Fax 062 51/702 64 44
info@concat.de, www.concat.de

top.media GmbH

Viktoriastraße 45,
65189 Wiesbaden
Tel. 06 11/411 10,
Fax 06 11/41 11 22
info@topmedia.de,
www.topmedia.de

Semico Computer GmbH

Daimlering 4, 65205 Wiesbaden
Tel. 061 22/700 60,
Fax 061 22/70 06 50
info@semico.de, www.semico.de

Carpe diem Kommunikations Technologie GmbH

Alte Schmelze 20,
65197 Wiesbaden
Tel. 06 11/95 17 50,
Fax 06 11/59 03 62
anfrage@carpediem.de,
www.carpediem.de

eSell GmbH

Halbergstraße 46,
66121 Saarbrücken
Tel. 06 81/88 39 30,
Fax 06 81/883 93 11
info@esell.de, www.esell.de

7**Cenit AG**

Industriestraße 52-54,
70565 Stuttgart
Tel. 07 11/78 25 30,
Fax 07 11/782 54 00 0
info@cenit.de,
www.cenit.de

Datagroup SE

Wilhelm-Schickard-Straße 7,
72124 Pliezhausen
Tel. 071 27/97 00 00,
Fax 071 27/97 00 33
kontakt@datagroup.de,
www.datagroup.de

Trigonova GmbH IT-Consulting

Madertal 15, 72401 Haigerloch
Tel. 074 74/95 18 00,
Fax 074 74/951 80 29
info@trigonova.de,
www.trigonova.de

am-Computersysteme GmbH

Seilerstr. 10, 72622 Nürtingen
Tel. 070 22/932 80-0
contact@am-computer.com,
www.am-computer.com

Inneo Solutions GmbH

IT-Campus 1, 73479 Ellwangen
Tel. 079 61/89 00
Inneo-de@inneo.com,
www.inneo.de

Bechtle AG

Bechtle Platz 1, 74172 Neckarsulm
Tel. 071 32/981 0,
Fax 071 32/981 80 00
kontakt@bechtle.com,
www.bechtde.com

TechniData IT AG

Emmy-Noether-Str. 9,
76131 Karlsruhe
Tel. 0721/35280-0
info@technidata-gruppe.de,
www.technidata-gruppe.de

Leitwerk AG

Im Ettenbach 13a,
77767 Appenweier-Urlaffen
Tel. 078 05/91 80,
Fax 078 05/91 82 000
info@leitwerk.de, www.leitwerk.de

MAIT GmbH

Berner Feld 10, 78628 Rottweil
Tel. 0741/1752-0,
Fax 0741/1752-200
info@mait.de, www.mait.de

8**Cancom Deutschland GmbH**

Erika-Mann-Str. 69, 80363 München
Tel. 089/54 05 40,
Fax. 089/540 54 51 19
info@cancom.de, www.cancom.de

Assistra Cloud Services GmbH

Blutenburgstr. 91 Rgb,
80634 München
Tel. 089/55 27 83 80,
Fax 089/55 05 15 85
sales@assistra-cloud.de,
www.assistra.de

MCE – ETV GmbH München

Helene-Wessel-Bogen 11,
80939 München
Tel. 089/318 56 20,
Fax 089/311 52 07
vertrieb@mce-etv.com,
www.mce-etv.com

microCAT Deutschland

Bunsenstrasse 3, 8
2152 Martinsried
Tel. 089/74 51 58-0
info@microcat.de,
www.microcat.de

PDV-Systeme GmbH

Geschäftsstelle München
Felix-Wankel-Straße 10,
85221 Dachau
Tel. 081 31/61 61-0,
Fax 081 31/61 61 29
muenchen@pdv-systeme.de,
www.pdv-systeme.de

Proact Deutschland GmbH

Südwestpark 43, 90449 Nürnberg
Tel. 09 11/309 99-0
info@proact.de, www.proact.de

tproneth The Storage Company GmbH & Co. KG

Zeppelinstraße 4, 82178 Puchheim
Tel. 089/44 23 10,
Fax 089/44 23 15 16
info@tpproneth.de,
www.tproneth.de

Bechtle Network und Security Solutions GmbH

Elisabeth-Schiemann-Bogen 3,
85716 Unterschleißheim
Tel. +49 89 1472764 100
info.bns@bechtde.com,
www.bechtde-network.com

Cyberport IT-Services

Petersbrunner Str. 8,
82319 Starnberg
Tel. 08151/7704-0, Fax
08151/7704-44
www.cyberport-it-services-
muenchen.de

NCS GmbH

Balthasar-Schaller-Str. 8,
86316 Friedberg
Tel. 08 21/74 850 0,
Fax 08 21/748 50 10
info@ncs.de, www.ncs.de

eSell Bayern GmbH

Flachsfeldstraße 21,
83607 Holzkirchen
Tel. 089/215 44 30 - 0
info@eSell.bayern,
www.eSell.bayern

NCS Ulm GmbH

Römerstraße 94
89077 Ulm
Tel. 0731 140223 00
info@ncsulm.de,
www.ncsulm.de

9**MR Datentechnik Vertriebs- und Service GmbH**

Emmericher Straße 13,
90411 Nürnberg
Tel. 09 11/52 14 70,
Fax 09 11/52 14 71 11
info@mr-daten.de,
www.mr-daten.de

SanData IT-Gruppe

Emmericher Straße 17,
90411 Nürnberg
Tel. 09 11/95 23 270,
Fax 09 11/95 23 221
info@sandata.de,
www.sandata.de

GL Consult Design & development GmbH

Hefnerplatz 10, 90402 Nürnberg
Tel. 09 11/941 16 90,
Fax 09 11/941 16 91
info@glconsult.com,
www.glconsult.com

HWS Informationssysteme GmbH

Robert-Bosch-Straße 1a,
91413 Neustadt/Aisch
Tel. 091 91/974076
info@hws-gruppe.de,
www.hws-informationssysteme.de

Sysob IT-Unternehmensgruppe GmbH & Co. KG

Kirchplatz 1, 93489 Schorndorf
Tel. 094 67/740 60,
Fax 094 67/740 62 90
info@sysob.de,
www.sysob.de



Bild: KI-generiert mit DALL-E, speicherguide.de

Zero-Trust war nie wichtiger

KI VERÄNDERT DIE SPIELREGELN DER CYBERSICHERHEIT

KI dreht das Tempo in der Cybersicherheit hoch. Angriffe laufen schneller, Session-Tokens können MFA aushebeln und autonome Agenten erweitern die Zahl privilegierter Identitäten. Gleichzeitig geraten Backup und Recovery stärker ins Visier. Zero-Trust wird damit zur Voraussetzung, um Zugriffe konsequent zu begrenzen und Schäden einzudämmen.



Karl Fröhlich
speicherguide.de

Klassische IT-Sicherheitsmodelle waren bisher vergleichsweise einfach gedacht: Wer draußen war, galt als potenziell gefährlich. Wer sich erfolgreich anmeldete und im internen Netz bewegte, bekam Vertrauen. Die-

ses Modell bricht zunehmend auseinander.

Cloud-Dienste, APIs, mobile Zugriffe und automatisierte Prozesse haben die klare Grenze zwischen innen und außen längst verwischt. Mit KI-Agen-

ten kommt eine weitere Ebene hinzu: Systeme handeln selbstständig, nutzen technische Identitäten und können in kurzer Zeit auf zahlreiche Ressourcen zugreifen. Gleichzeitig reichen gestohlene Zugangsdaten oder gültige

Session-Tokens aus, um legitime Identitäten für Angriffe zu missbrauchen.

Damit wird nicht nur die Abwehr schwieriger. Vor allem gewinnt die Frage an Bedeutung, wie weit ein einzelner kompromittierter Zugang überhaupt kommen kann. Genau hier setzt Zero-Trust an: Ein erfolgreicher Login schafft kein dauerhaftes Vertrauen. Zugriffe bleiben auf bestimmte Ressourcen, Rechte und den jeweiligen Kontext begrenzt.

Der erfolgreiche Login schafft kein dauerhaftes Vertrauen

Viele Sicherheitskonzepte funktionieren noch immer wie eine Eingangskontrolle. Wer Benutzername, Passwort und gegebenenfalls einen zweiten Faktor erfolgreich präsentiert, erhält zunächst einen Vertrauensvorschuss. Gestohlene Session-Tokens zeigen, wie brüchig dieses Modell geworden ist.

Nach einer erfolgreichen Anmeldung erzeugen viele Dienste ein Token, das bestätigt, dass der Benutzer bereits authentifiziert wurde. Dadurch muss er sich nicht bei jedem Zugriff erneut mit Passwort und MFA (Multi-Factor Authentication) anmelden. Gelangt dieses Token jedoch in die Hände eines Angreifers, kann dieser unter Umständen eine bestehende Sitzung übernehmen, ohne dass erneut eine MFA-Abfrage erfolgt. Genau solche Token-Replay-Angriffe dokumentieren die zugrunde liegenden Sicherheitsberichte.

MFA bleibt deshalb unverzichtbar, reicht allein aber nicht aus. Identitätssicherheit darf nicht bei der Anmeldung enden. Eine erfolgreiche Authentifizierung bestätigt zunächst den Zugang zu einer Sitzung. Sie legitimiert nicht automatisch jede weitere Aktion innerhalb dieser Sitzung.

Zero-Trust macht diese Trennung zum Prinzip. Zugriff wird nicht pauschal gewährt, sondern abhängig von Identität, Ressource, Kontext und angeforderter Aktion bewertet. Gerät, Anwendung, Standort, Zeitpunkt, Session-Verlauf und auffälliges Verhalten können dabei ebenso relevant sein wie die ursprüngliche Anmeldung.

KI macht übergroße Rechte gefährlicher

Ein kompromittiertes Konto war schon immer problematisch. Mit automatisierten Agenten steigt jedoch die Geschwindigkeit, mit der zu weit gefasste Berechtigungen ausgenutzt werden können. Ein Mensch arbeitet sich nacheinander durch Systeme und Datenbestände. Ein Agent kann dieselben Rechte schneller, wiederholbar und teilweise parallel einsetzen.

Damit steigt der mögliche Schaden durch schlecht geschnittene Rollen und universelle Zugänge. Least Privilege wird von einer Best Practice zur Voraussetzung für beherrschbare Automatisierung. Jede Identität sollte nur die Rechte besitzen, die sie für ihre konkrete Aufgabe benötigt.

Das gilt besonders für KI-Agenten. Sobald sie E-Mails durchsuchen, Do-

kumente verändern, Cloud-Dienste ansprechen, Quellcode bearbeiten oder Datenbanken abfragen, werden sie zu technischen Identitäten mit teils weitreichenden Rechten. Diese Zugänge müssen deshalb mindestens so konsequent beschränkt werden wie klassische Dienstkonten und andere automatisierte Prozesse.

Bei OpenAI und Anthropic sind mehrere Fälle dokumentiert, in denen Agenten während Trainings- oder Sicherheitstests die Grenzen ihrer vorgesehenen Umgebung überschritten. Dafür braucht ein KI-System keine eigene Absicht. Es genügt, wenn ein Ziel vorgegeben ist, Berechtigungen zu weit gefasst sind und der Agent einen technisch möglichen Weg als zulässig interpretiert.

Für die Sicherheitsarchitektur folgt daraus eine klare Konsequenz: KI-



Zero Trust basiert auf klaren Regeln für Identitäten, Zugriffe und Systeme. Die sieben Kernprinzipien schaffen dafür den gemeinsamen Sicherheitsrahmen.



Agenten benötigen eigene technische Identitäten, eng begrenzte Rechte und nachvollziehbare Aktionen. Gemeinsam genutzte Konten und universelle Zugangsschlüssel passen nicht zu einem Zero-Trust-Modell.

Maschinenidentitäten rücken ins Zentrum

In modernen IT-Umgebungen greifen längst nicht mehr nur Menschen auf Systeme zu. Anwendungen, APIs, Service-Accounts, Skripte, Automatisierungsplattformen und KI-Agenten kommunizieren laufend miteinander. Mit jedem zusätzlichen Dienst wächst die Zahl nichtmenschlicher Identitäten.

Solche technischen Zugänge können weitreichende Rechte besitzen. Besonders kritisch sind API-Keys. Viele Cloud- und KI-Dienste akzeptieren sie direkt als Zugangsnachweis. Wer einen gültigen Key besitzt, benötigt unter Umständen weder Passwort noch MFA.

Dauerhaft gültige API-Keys können deshalb wie Generalschlüssel wirken. Sie sollten möglichst durch kurzlebige Zugangsdaten ersetzt oder zumindest funktional, zeitlich und hinsichtlich ihres Nutzungsumfangs begrenzt werden. Auffällige Zugriffsmuster, unge-

wöhnliche Datenmengen und sprunghaft steigende Nutzung gehören ebenso überwacht wie klassische Benutzeraktivitäten. Der zugrunde liegende Okta-Bericht dokumentiert neben gestohlenen Session-Tokens auch noch gültige API-Keys in Info-stealer-Daten.

Zero-Trust verschiebt damit den Schwerpunkt von der Frage, wo sich ein System befindet, hin zu der Frage, welche Identität welche Ressource unter welchen Bedingungen nutzen darf. Diese Logik passt zu Cloud-, SaaS- und Agenten-Umgebungen besser als ein klassisches Innen-und-Außen-Modell.

Netzwerkgrenzen reichen nicht mehr aus

Netzwerksegmentierung bleibt wichtig, kann die heutige Infrastruktur aber nicht mehr allein absichern. Moderne Anwendungen verteilen sich über Cloud-Dienste, SaaS-Plattformen, APIs, Container und lokale Systeme. Daten und Prozesse überschreiten laufend traditionelle Netzwerkgrenzen.

Deshalb darf ein interner Standort keinen Vertrauensbonus mehr erzeugen. Auch ein authentifiziertes System benötigt nicht automatisch Zugriff auf andere Anwendungen oder Datenbe-

stände. Mikrosegmentierung, restriktive Kommunikationspfade und ressourcenbezogene Berechtigungen begrenzen den Bewegungsraum, wenn eine Identität kompromittiert wurde.

Das Prinzip gilt für Menschen ebenso wie für Agenten. Ein Entwicklungsagent braucht keinen Zugriff auf Produktivdaten, nur weil er im selben Cloud-Tenant arbeitet. Ein System, das Anwendungen aktualisiert, benötigt keine Berechtigung zum Löschen von Backups. Und ein Dienst, der Daten lesen soll, braucht nicht automatisch Schreibrechte.

Backup und Recovery brauchen eigene Vertrauensgrenzen

Cyber-Resilienz endet nicht beim Schutz der Produktion. Angreifer nehmen auch Backup- und Recovery-Umgebungen ins Visier. Wer ein Unternehmen nachhaltig erpressen oder schädigen will, versucht nicht nur Produktivdaten zu verschlüsseln, sondern auch den Weg zurück abzuschneiden.

Besonders gefährlich sind manipulierte Sicherungen und Wiederherstellungsprozesse. Anthropic beschreibt Angriffe, bei denen auch die Backup-

Umgebung betroffen war und manipulierte Sicherungen eine wiederhergestellte Umgebung erneut kompromittieren konnten.

Backup und Recovery sollten deshalb als eigene Sicherheitsdomänen behandelt werden. Weitreichende Rechte im Produktivsystem dürfen nicht automatisch für Sicherungen, Snapshots oder Recovery-Plattformen gelten. Getrennte Identitäten, eingeschränkte Administrationspfade, unveränderbare Sicherungskopien und geschützte Protokolle reduzieren das Risiko, dass ein einzelner kompromittierter Zugang sämtliche Rückfallebenen erreicht.

Damit wird Zero-Trust direkt zu einem Baustein der Cyber-Resilienz. Das Konzept verhindert nicht zwingend den ersten erfolgreichen Zugriff. Es begrenzt aber, welche Ressourcen ein kompromittierter Benutzer, Dienst oder Agent anschließend erreichen und verändern kann.

»Assume Breach« beschreibt die Realität

Eine der zentralen Ideen hinter Zero-Trust lautet »Assume Breach«: Die Sicherheitsarchitektur geht davon aus, dass ein Angreifer bereits innerhalb der Umgebung sein könnte. Was lange übervorsichtig klang, entspricht heute zunehmend der Praxis.

Ein Benutzer kann legitim sein, sein Rechner aber kompromittiert. Eine Sitzung kann korrekt authentifiziert worden sein, das Session-Token später jedoch gestohlen werden. Ein API-Key kann gültig sein und trotzdem von einem Angreifer verwendet werden. Ein KI-Agent kann zum Unternehmen gehören und dennoch eine Aktion ausführen, die nie vorgesehen war.

Zero-Trust versucht nicht, diese Unsicherheit vollständig zu beseitigen.

Das Ziel besteht darin, ihre Auswirkungen klein zu halten. Dafür müssen Identitäten eindeutig zugeordnet, Berechtigungen eng geschnitten, Sitzungen überwacht und kritische Aktionen zusätzlich abgesichert werden.

Besonders wichtig ist die Trennung von Rollen. Ein kompromittierter Benutzer oder Agent darf nicht gleichzeitig Anwendungen administrieren, Daten exportieren, Backups löschen und Protokolle verändern können. Je stärker Unternehmen Prozesse automatisieren, desto wichtiger werden solche Grenzen.

Zero-Trust wird durch KI wichtiger, nicht überflüssig

Der KI-Boom bestätigt damit ein Sicherheitsprinzip, das seit Jahren bekannt ist. Eine korrekt authentifizierte Identität ist noch lange keine vertrauenswürdige Identität. Entscheidend ist, welche Aktion sie auf welcher Ressource ausführen darf und ob dieses Recht in diesem Moment noch gerechtfertigt ist.

Mit autonomen Agenten wächst die Zahl der Identitäten, die selbstständig handeln können. Gleichzeitig machen KI-gestützte Abläufe bekannte Angriffe schneller und skalierbarer. Anthropic dokumentiert bereits Fälle, in denen einzelne Operatoren mehrere Opfer parallel bearbeiten und Agenten operative Angriffsschritte weitgehend selbstständig übernehmen konnten.

Zero-Trust entwickelt sich deshalb vom Architekturkonzept zur Voraussetzung für beherrschbare Automatisierung. Wer Rechte klein hält, Maschinenidentitäten genauso streng behandelt wie Benutzerkonten und Backup sowie Recovery in dieselbe Sicherheitslogik einbezieht, begrenzt den Schaden dort, wo klassische Perimeter längst nicht mehr greifen. ■

Weiterführende Links:

- 🔗 KI außer Kontrolle: Warum freiwillige Regeln nicht reichen
- 🔗 Anthropic: Cyberangriffe eskalieren innerhalb weniger Stunden
- 🔗 OpenAI-Agenten griffen RubyGems schon vor Hugging Face an
- 🔗 KI-Zugänge: Schwarzmarkt umgeht MFA mit Session-Tokens



speicherguide.de

storage-magazin.de
E-MAGAZIN VON speicherguide.de

Zero Trust in der Praxis
Strategien, Tools und Best Practices für Security, Backup und Recovery
1/2027

Immer up to date mit dem Newsletter von speicherguide.de

- 📧 Aktuelle News, Trends und Analysen zu Zero Trust, Security, Backup und Recovery.
- 📄 Praxisnahe Fachartikel, Best Practices und Tool-Tipps.
- 🔔 Wissen, das Sie weiterbringt – kompakt, relevant.

Jetzt Newsletter abonnieren ➔

Infrastruktur- und Storage-Kosten 2027

WENN DAS BUDGET NICHT MEHR REICHT

Die Preise für Server und Speicher steigen, Lieferzeiten und Verfügbarkeit bleiben schwer kalkulierbar. Für Unternehmen wird es immer schwieriger, ihre IT-Infrastruktur zu modernisieren. Selbst notwendige Investitionen stehen auf dem Prüfstand.



Karl Fröhlich
speicherguide.de

Die Frage, ob ein neuer Server 25.000 oder 30.000 Euro kostet, wirkt inzwischen fast nostalgisch. Ein IT-Administrator berichtete uns im Gespräch von einem Server, der 2025 rund 28.000 Euro gekostet habe. Für eine vergleichbare Ausstattung würden heute 178.000 Euro aufgerufen. Die genauen Konfigurationen liegen der Redaktion nicht vor. Der geschilderte Preissprung ist daher nicht unabhängig überprüfbar.

Dass Server-Preise erheblich gestiegen sind, lässt sich am *HPE ProLiant DL380 Gen11* mit 64 GByte RAM und 1,92 TByte Speicher nachvollziehen: Laut **idealo.de** kostete dieser zwischenzeitlich 160 Prozent mehr als zum Tiefstpreis. Aktuell beträgt der Aufschlag noch 84 Prozent. Der Preisverlauf eines einzelnen Modells mag nicht repräsentativ sein, die Entwicklung ist produktübergreifend relativ identisch.

Preissprünge statt Planungssicherheit

KI-Rechenzentren und Cloud-Anbieter sichern sich große Speicherkontingente. Hersteller bevorzugen Produkte mit hohen Margen. Für das vierte Quartal 2026 er-

wartet **TrendForce** weitere Preissteigerungen gegenüber dem Vorquartal: 10 bis 15 Prozent bei konventionellem DRAM, 15 bis 20 Prozent bei NAND-Flash und 23 bis 28 Prozent bei Enterprise-SSDs.

Für den Mittelstand ist nicht nur der höhere Preis ein Problem. Bereits freigegebene Budgets reichen unter Umständen nicht mehr aus, Liefertermine bleiben unsicher. Hinzu kommen die Kosten für herstellergebundene Komponenten, Lizenzen und Wartungsverträge. Gerade bei Erweiterungen haben Kunden oft wenig Spielraum, auf günstigere Alternativen auszuweichen.

Auch nach der KI-Blase bleiben Preise hoch

Speicherpreise können durchaus wieder sinken. DRAM und NAND haben bereits mehrere ausgeprägte Preiszyklen durchlaufen. Auch eine mögliche KI-Blase wird immer wieder diskutiert.

Die speicherguide.de-Redaktion bezweifelt, dass alle geplanten Rechenzentren tatsächlich gebaut werden. Manche Projekte dürften an fehlenden Standorten, mangelnder Stromversorgung, hohen Energiekosten oder der Finanzierung scheitern. Damit sollten bereits reservierte Speicherkapazitäten wieder verfügbar werden.

Ob dadurch die Preise deutlich sinken, steht auf einem anderen Blatt. Hersteller und Anbieter haben wenig Interesse daran, ihre hohen Preise freiwillig aufzugeben. Solange die Nachfrage hoch bleibt, gibt es für sie wenig Anlass zu größeren Nachlässen. Erst ein Überangebot könnte den Wettbewerb und damit die Preise wieder stärker unter Druck setzen. Eine baldige Rückkehr zum früheren Preisniveau ist deshalb kaum zu erwarten.

Sparen, aber nicht an der falschen Stelle

Unternehmen müssen deshalb genauer priorisieren. Welche Systeme müssen wegen auslaufendem Support, Sicherheitsrisiken oder fehlender Leistung ersetzt werden? Wo reichen gezielte Erweiterungen, eine Konsolidierung oder eine bessere Verteilung der Daten auf vorhandene Speicherklassen?

Entscheidend ist, nicht an der falschen Stelle zu sparen. Eine verschobene Erweiterung mag verkraftbar sein. Wer dagegen Investitionen in Backup, Wiederherstellung oder geschäftskritische Systeme auf unbestimmte Zeit verschiebt, riskiert deutlich höhere Folgekosten als die eingesparten Hardware-Kosten.



Doc Storage.

Jetzt auch auf **YouTube**.

Sicherheit
Backup
Storage
KI
Resilienz

speicherguide.de
Das Storage-Magazin

News Storage Backup Datacenter Infrastrukturen Management

Wissen / Doc Storage

Berlin – das EDV-Shithole... 18.09.2026

BERLINER IT: LÖSUNG AB 2027 HACKER KAMEN FRÜHER
Doc. TEC. STORAGE

Berlin wusste seit Jahren, dass sein Landesnetz für Verschlusssachen nicht ausreichend gerüstet war. Trotzdem blieb es bei Zwischenlösungen, Einzelrechnern und Papierakten. Dann kamen die Angreifer früher als die geplante Lösung. Doc Storage kommentiert Behörden-IT zwischen Versäumnissen, Aktionismus und erstaunlicher Gelassenheit.

US-Produkte: Heute ist ein guter Tag Abhängigkeiten zu reduzieren 21.03.2025

US-PRODUKTE: JETZT KONSEQUENZEN ZIEHEN
Doc. TEC. STORAGE

Annähernd unsere gesamte digitale Infrastruktur ist der US-Politik ausgeliefert. Auch wenn es unbequem ist, IT-Abteilungen müssen damit anfangen, sich von dieser Abhängigkeit zu befreien. Doc Storage rät dazu, es sich

Doc. Storage

Datacenter
Storage
Backup
IT-Sicherheit

Derselbe Doc. Neues Format.



Kanal entdecken →