storage-magazin.de

Eine Publikation von speicherguide.de

1 | 2026

- **STRATEGIE**
  Chefsache: Digitale Datensouveränität
- **TECHNIK**
  Storage für KI neu denken
- **SICHERHEIT**
  Cyber-Resilienz und Cybersicherheitspflichten

40 Seiten
geballtes
Storage-Wissen

Einkaufsführer Storage 2026

Bild: speicherguide.de via DALL-E

Schnelle All-Flash-Speicher für das Rechenzentrum

Veeam Immutable Backup:
Jetzt auch auf EUROstor Server mit Open-E

ES-8700 12 Slot Server mit Open-E JovianVHR Software

Beispielkonfiguration:
2 HE Rack Server mit 16-CORE AMD CPU,
192 GB RAM, 2 x 25 GbE Ports,
voll bestückt mit 10 x 14 TB NL-SAS Disks,
damit ca. 91,7 TiB verfügbare Kapazität
bei einem RAID-Z2 (entspricht RAID6),
Open-E JovianVHR vorinstalliert
auf M.2 SSDs,
3 Jahre Open-E Standard Support

€ 10.290,-
exkl. MwSt.

€ 12.245,10
inkl. MwSt.

Für alle Veeam-Nutzer, die das immutable Backup auf einem „Linux Hardened Repository" als **Schutz vor Ransomware** nutzen wollen.

Open-E JovianVHR ist eine Veeam qualifizierte Softwareversion von Open-E, die die **Vorteile des ZFS Filesystems** mit der **Unveränderlichkeit der Daten** durch das Veeam Linux Hardended Repository verbindet.

Die Lizenz ist kostenlos, und der obligatorische Support durch Open-E ist zu moderaten Preisen erhältlich.

Ebenso erhältlich bei EUROstor:

- **ES-8700J Storageserver** mit **Open-E JovianDSS** für NAS (NFS und CIFS/SMB), iSCSI und optional FC.
- auch als **Active/Active Cluster** lokal oder als **Metro-Cluster** über zwei Standorte
- **OODP Server** (On & Off-Site Data Protection) als **snapshotbasierte Sicherung** an einen anderen Standort

Gerne erstellen wir ein maßgeschneidertes Angebot für Sie.

Für alle Systeme gilt:

- **ZFS 2.0 Filesystem**: maximale Datenintegrität und Schutz vor „Stealth Errors" durch Check-Summen-Prüfung und Disk-Scrubbing.
- umfangreiche Snapshot- und Replikationsfunktionen ohne Zeitverlust und vorreservierte Kapazität
- Kompression, Deduplizierung & Thin Provisioning
- eine **intuitive Web-GUI** erlaubt einfaches Management ohne Spezialkenntnisse.

Alle Storage-Systeme aus einer Hand:

EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unser Portfolio umfasst RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, allgemein einsetzbaren Servern, z.B. für die Server-Virtualisierung.

Registrieren Sie sich einfach unter www.EUROstor.com/Newsletter,

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt – E-Mail: Info@EUROstor.com – Tel.: +49 (0)711 70 70 91 70

Editorial

Karl Fröhlich
Chefredakteur
speicherguide.de

SOUVERÄNITÄT – VOM RANDTHEMA ZUM STRATEGISCHEN MUSS

Stellen Sie sich vor: Ihre wichtigsten Unternehmensdaten liegen sicher im Rechenzentrum in Frankfurt. Doch plötzlich entscheidet ein US-Gericht, dass diese Daten herausgegeben werden müssen. Was vor Kurzem noch undenkbar schien, ist heute längst Realität.

Die IT-Welt ist unberechenbar geworden. Gesetze wie der US-Cloud-Act und neue Vorgaben zu internationalen Datentransfers stellen europäische Unternehmen vor nie dagewesene Herausforderungen. Selbst wenn Daten physisch in Deutschland gespeichert sind – die Kontrolle darüber kann im Ernstfall entgleiten, ohne dass man Sie davon in Kenntnis setzt.

Daten-Souveränität: Plötzlich Chefsache

Mit der aktuellen US-Regierung geraten nationale Sicherheitsinteressen und Zugriffsrechte weltweit stärker in den Fokus. Europa reagiert mit NIS-2, strengeren Aufsichtsanforderungen und Souveränitäts-Programmen. Trotzdem dominieren US-Hyperscaler den Markt, und viele ihrer »Sovereign Cloud«-Angebote bleiben in der Logik amerikanischer Gesetze gefangen. Für IT-Abteilungen fühlt sich das an, als würde auf einem Teppich geplant, der jederzeit weggezogen werden kann.

Was bedeutet das für Ihre Storage-Strategie?

Storage-Souveränität entwickelt sich gerade vom »nice to have« zur strategischen Pflicht. Mittelständische Unternehmen und IT-Abteilungen prüfen heute genau: Welche Daten dürfen noch in die US-Cloud? Wann ist ein europäisches Rechenzentrum, ein regionaler Dienstleister oder gar das eigene Rack die bessere Wahl? Lösungen »made in EU«, On-Prem-Object-Storage, S3-Systeme und hybride Szenarien gewinnen an Bedeutung. Entscheidend ist: Wer hält die Schlüssel zu Ihren Daten? Wer hat operativen Zugriff? Und wie flexibel sind Sie, wenn Sie Ihre Strategie plötzlich anpassen müssen?

Unsere Aufgabe: Orientierung und konkrete Hilfestellung

Die IT-Welt ist nicht ruhiger geworden – sie ist geopolitischer. Die gute Nachricht: Souveränität ist kein abstraktes Schlagwort mehr, sondern rückt auf die Vorstandsagenda und prägt die IT-Strategie. Genau hier setzt unser neues eMagazine an. Wir zeigen Ihnen, welche Optionen es im Bereich Storage und Dateninfrastruktur gibt, wie Sie Compliance sichern, Kosten im Blick behalten – und dennoch flexibel für die nächste Überraschung bleiben.

Lassen Sie uns gemeinsam Lösungen für diese neue Realität entwickeln. Wir wünschen Ihnen viele Impulse und praxisnahe Orientierung beim Lesen dieser Ausgabe!

Ihr Karl Fröhlich
Chefredakteur, speicherguide.de

Bild: speicherguide.de via DALL-E

Echte Souveränität für deutsche Firmen mehr als ein Marketing-Versprechen

BITKOM WARNT: DEUTSCHE IT HÄNGT AM TROPF AUSLÄNDISCHER ANBIETER

SEITE 5

Bitkom-Zahlen zeigen eine hohe digitale Abhängigkeit der deutschen Wirtschaft. Neun von zehn Firmen sehen sich auf Importe angewiesen, mehr als die Hälfte könnte ohne Hardware, Software und Cloud-Services aus dem Ausland höchstens ein Jahr weiterarbeiten. Während die Abhängigkeit von USA, China und Taiwan wächst, sinkt zugleich das Vertrauen in diese Partner.

Vom Nischenprodukt zum Standard: All-Flash-Speicher im Überblick

SCHNELLER STORAGE FÜR DAS RECHENZENTRUM

Bild: speicherguide.de und die jeweiligen Hersteller via DALL-E

SEITE 24

Studien-Update 2025: Kapazitäten, Standorte, Energie, Politik

BITKOM-STUDIE: KI MACHT DRUCK AUF DEUTSCHLANDS RECHENZENTREN

Bild: speicherguide.de via DALL-E

SEITE 34

Übersicht
Storage-Anbieter

SEITE 9

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

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

Redaktion:
Michael Baumann, Karl Fröhlich, Uli Neiss
Schlussredaktion:
Brigitte Scholz

Titelbild:
speicherguide.de via DALL-E

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

Mediaberatung:
Bettina Röber
Tel. 0177-8487001
E-Mail: broeber@speicherguide.de

Echte Souveränität für deutsche Firmen mehr als ein Marketing-Versprechen

BITKOM WARNT:
DEUTSCHE IT HÄNGT AM TROPF AUSLÄNDISCHER ANBIETER

Bitkom-Zahlen zeigen eine hohe digitale Abhängigkeit der deutschen Wirtschaft. Neun von zehn Firmen sehen sich auf Importe angewiesen, mehr als die Hälfte könnte ohne Hardware, Software und Cloud-Services aus dem Ausland höchstens ein Jahr weiterarbeiten. Während die Abhängigkeit von USA, China und Taiwan wächst, sinkt zugleich das Vertrauen in diese Partner.

Karl Fröhlich
speicherguide.de

Hardware aus China, Cloud- und KI-Plattformen aus den USA, Chips aus Taiwan, Industrieroboter aus Südkorea – ein Großteil der digitalen Wertschöpfung deutscher Unternehmen beruht auf importierten Technologien. In einer Befragung unter mehr als 600 Unternehmen ab 20 Mitarbeitenden ermittelt der Digitalverband **Bitkom**, dass 96 Prozent digitale Technologien oder Services aus dem Ausland beziehen. 89 Prozent dieser Firmen stufen sich selbst als abhängig ein, gut die Hälfte davon sogar als stark abhängig. 57 Prozent geben an, ohne Digitalimporte höchstens zwölf Monate wirtschaftlich überleben zu können. Nur vier Prozent halten sich langfristig für überlebensfähig, wenn die Zuflüsse von Hardware, Software und Services versiegen.

Bitkom-Präsident **Dr. Ralf Wintergerst** fordert daher: »Deutschland und Europa müssen sich aus einseitigen Abhängigkeiten befreien und ihre digitale Zukunft selbst in die Hand nehmen. Europa muss seine digitale Souveränität mit mehr Entschlossenheit entwickeln. Wir müssen Europa zu einem Ort machen, an dem digitale Technologien nicht nur genutzt, sondern auch entwickelt und in wettbewerbsfähige Produkte und Dienstleistungen übersetzt werden.«

USA und China als zentrale Lieferländer

Besonders deutlich wird die Konzentration auf wenige Herkunftsländer. 67 Prozent der Unternehmen importieren häufig digitale Technologien aus den USA, weitere 23 Prozent in Einzelfällen. Damit zählen die Vereinigten Staaten für neun von zehn Firmen, die Digitalimporte nutzen, zu den Handelspartnern. Aus China beziehen 58 Prozent häufig und 25 Prozent gelegentlich digitale Güter. In der Praxis hängen damit zentrale Bausteine vieler IT- und Produktionsumgebungen an genau diesen beiden Märkten.

Eine Schlüsselrolle spielt Taiwan. 21 Prozent der Unternehmen importieren häufig, 24 Prozent in Einzelfällen digitale Technologien und Leistungen von der Insel. Nahezu die Hälfte der importierenden Firmen sieht sich von Taiwan abhängig, 26 Prozent sogar stark. Wintergerst warnt: »Die deutsche Wirtschaft ist vergleichsweise stark von Taiwan abhängig, da Schlüsselindustrien wie die Automobil- und Elektronikbranche auf dort produzierte Hochleistungs-Chips angewiesen sind. Chinas Aggressionen gegen Taiwan bedrohen deshalb direkt die Lieferketten und Produktionskapazitäten in Deutschland.« Für viele industrielle Kernbranchen ergibt sich damit ein hochkonzentriertes Halbleiter-Risiko.

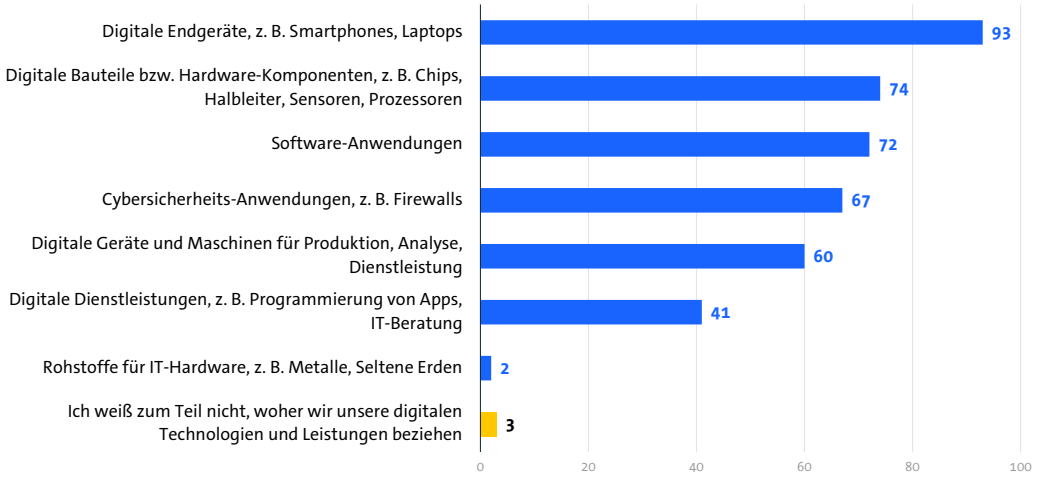
»Wir müssen Europa zu einem Ort machen, an dem digitale Technologien nicht nur genutzt, sondern auch entwickelt und in wettbewerbsfähige Produkte und Dienstleistungen übersetzt werden.«

Bild: Bitkom

Dr. Ralf Wintergerst, Bitkom

Ohne Digital-Importe geht es nicht

Welche digitalen Technologien oder Leistungen bezieht Ihr Unternehmen aus dem Ausland?



96% der Unternehmen beziehen digitale Technologien oder Leistungen aus dem Ausland.

Basis: Alle befragten Unternehmen (n=605) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

bitkom

Begrenzte Diversifizierung über Japan, EU und Vereinigtes Königreich

Ganz ohne Diversifizierung sind die Unternehmen dennoch nicht. Japan ist für zwölf Prozent ein häufiger und für 31 Prozent ein gelegentlicher Lieferant digitaler Technologien. Frankreich liefert bei zehn Prozent häufig und bei 20 Prozent in Einzelfällen digitale Güter. Für die übrige EU liegen die Werte bei 16 und 28 Prozent, für das Vereinigte Königreich bei elf und 19 Prozent. Russland spielt praktisch keine Rolle mehr, nur ein Prozent der Firmen nennt die Russische Föderation als Bezugsquelle für digitale Technologien.

Deutschland im Abhängigkeitsmodus

Auf der Makroebene sehen 93 Prozent der Unternehmen Deutschland insgesamt technologisch stark oder eher abhängig von digitalen Leistungen aus dem Ausland. Nur zehn Prozent erwarten, dass sich diese Abhängigkeit in den kommenden fünf Jahren verringert, fast zwei Drittel rechnen sogar mit einer Zunahme. Parallel sinkt das Vertrauen in zentrale Partnerländer. Besonders die USA geraten in den Fokus. Neben geopolitischen Spannungen verweisen die Unternehmen auf rechtliche Rahmenbedingungen wie den US Cloud Act und auf Debatten um Datenschutz und staatliche Zugriffe auf Daten in ausländischen Cloud-Infrastrukturen. Bei China stehen politische Einflussnahme, Exportkontrollen und das Risiko von Lieferunterbrechungen im Vordergrund.

Vertrauen in Europa, Skepsis gegenüber USA und China

Die Diskrepanz zwischen realen Importströmen und Vertrauensniveau zeigt ein Blick auf das Bitkom-Ranking. Am meisten Vertrauen genießen Frankreich, Japan und andere EU-Staaten. 76 Prozent der Unternehmen äußern Vertrauen in Frankreich, 72 Prozent in Japan und 68 Prozent in die übrige EU. Dahinter folgen das Vereinigte Königreich mit 58 Prozent, Indien mit 45 Prozent und Südkorea mit 40 Prozent. In die USA haben dagegen nur noch 38 Prozent Vertrauen, 60 Prozent vertrauen den Vereinigten Staaten wenig oder gar nicht. China schneidet noch schlechter ab. 70 Prozent bringen dem Land wenig oder kein Vertrauen entgegen, nur 26 Prozent äußern Vertrauen.

Messbar ist zudem der Einfluss der politischen Entwicklungen in den USA. Ein Drittel der Unternehmen berichtet von sehr negativen, weitere 46 Prozent von eher negativen direkten oder indirekten Auswirkungen der Präsidentschaft Donald Trumps auf das eigene Geschäft. Für 19 Prozent ergaben sich bislang keine spürbaren Veränderungen, positive Effekte meldet kein einziges Unternehmen. Betrachtet man nicht das eigene Unternehmen, sondern Deutschland als Ganzes, bewerten allerdings 52 Prozent die USA weiterhin als verlässlichen Partner.

Weiterführende Infos:

Lesen Sie die detaillierte Langfassung der Bitkom-Studie »Europas Weg in die digitale Souveränität« auf speicherguide.de

DATACORE™

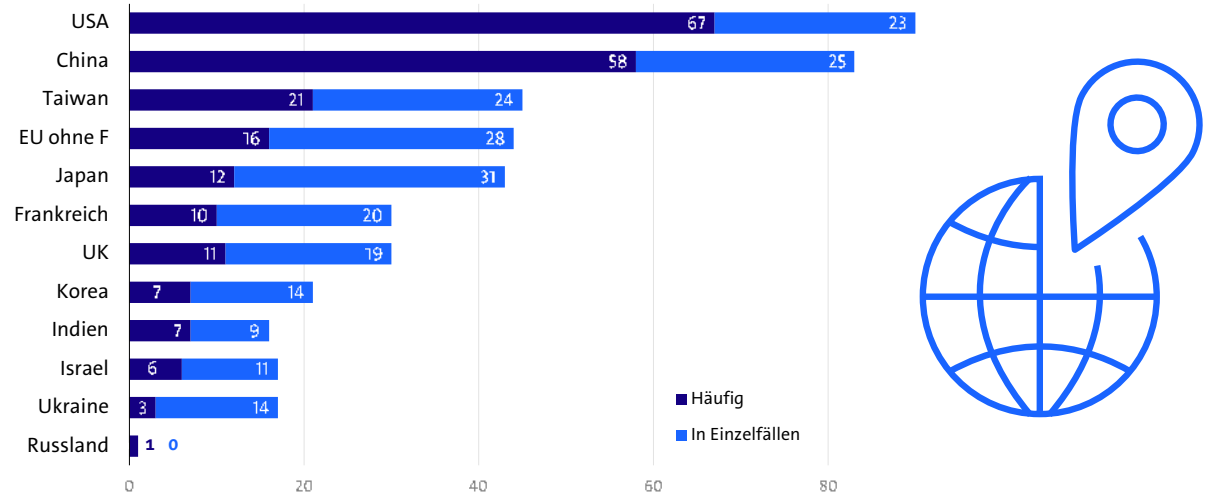
Solving **Data Challenges** *at* **Every Level**

More Solutions. *More Possibilities.* **One DataCore.**

Your Data, Our Priority

USA und China sind die wichtigsten Herkunftsländer

Aus welchen Ländern bzw. Regionen beziehen Sie digitale Technologien bzw. Leistungen?



Basis: Unternehmen, die digitale Technologien bzw. Leistungen aus dem Ausland beziehen (n=579) | Quelle: Bitkom Research 2025

bitkom

Gesellschaftlicher Rückhalt für mehr digitale Unabhängigkeit

Die Wahrnehmung digitaler Abhängigkeiten ist nicht auf die Wirtschaft beschränkt. In einer weiteren Bitkom-Umfrage halten 44 Prozent der Bundesbürgerinnen und Bundesbürger Deutschland für sehr abhängig von digitalen Technologieimporten, 50 Prozent für eher abhängig. 98 Prozent sehen es als wichtig an, dass Deutschland bei zentralen digitalen Technologien unabhängiger wird. Wintergerst fasst zusammen: »Die Menschen in Deutschland haben den Ernst der Lage verstanden. Fast alle wünschen sich mehr Unabhängigkeit bei digitalen Schlüsseltechnologien. Das Vertrauen in Partner wie die USA oder China hat zuletzt stark gelitten. Die Stärkung unserer digitalen Souveränität und Wettbewerbsfähigkeit gehört in den kommenden drei Jahren der Legislaturperiode ganz oben auf die Agenda.«

Risiken durch Handelskonflikte und Tech-Auflagen

Beim Blick nach vorne spielen Risiken aus Sicht der Unternehmen eine zentrale Rolle. 99 Prozent sehen zusätzliche finanzielle Belastungen durch Strafzölle oder Sanktionen als Risiko, 56 Prozent fürchten neue Exportbeschränkungen, 49 Prozent einen möglichen Austritt der USA aus internationalen Organisationen wie der NATO oder der WTO. Digitale Einzelrisiken fallen demgegenüber etwas weniger ins Gewicht. 49 Prozent sorgen sich vor einem Verlust des Zugangs zu Software- und Plattformdiensten, 41 Prozent vor einem erzwungenen Abfluss sensibler Unternehmensdaten an US-Behörden, 37 Prozent vor erschwertem Zugang zu Chips oder KI-Systemen. Einschränkungen bei Cloud-Services bewerten nur 14 Prozent als wesentliches Risiko.

Was Unternehmen und Politik jetzt liefern sollen

Als Konsequenz fordern 94 Prozent der Unternehmen verstärkte Investitionen in digitale Schlüsseltechnologien. 62 Prozent plädieren für den Aufbau europäischer Hyperscaler, also großer Cloud-Anbieter in europäischer Hand. Wintergerst formuliert die Grundbedingung so: »Nur wer über eigene Kompetenzen verfügt, kann international auf Augenhöhe agieren – und dafür muss Deutschland seine Position gezielt stärken.« Bitkom nennt in diesem Zusammenhang den Ausbau leistungsfähiger Cloud- und Rechenzentrums-Infrastrukturen in Europa, eigene Fähigkeiten bei Künstlicher Intelligenz, Quantum-Computing, Industrial Metaverse und IT-Sicherheit sowie den Auf- und Ausbau der Chip-Fertigung in Deutschland.

Als weiterer Baustein gilt die *European Digital Identity Wallet*. Sie soll Bürgerinnen und Bürgern sowie Unternehmen ermöglichen, Identitätsdaten und digitale Nachweise sicher, selbstbestimmt und grenzüberschreitend zu verwalten. »Die EUDI-Wallet ist ein zentrales Instrument zur Stärkung der digitalen Souveränität«, betont Bitkom. Sie soll Abhängigkeiten von proprietären Identitäts-Ökosystemen großer internationaler Plattform-Anbieter verringern.

Digitale Souveränität sichert Handlungsfähigkeit

Am Ende steht eine klare Botschaft: Digitale Souveränität ist kein abstraktes Politikkonzept, sondern eine Frage der operativen Handlungsfähigkeit von Unternehmen und Volkswirtschaften. Wer seine digitalen Lieferketten nicht kennt und einseitige Abhängigkeiten nicht reduziert, bleibt anfällig für politische Schocks, Handelskonflikte und technologische Blockaden. ■

DataCore Software

www.datacore.com/de/

Sitz der Gesellschaft:
USA

Niederlassungen in Deutschland:
Unterföhring bei München

Jahr der Gründung:
1998

Zielgruppe:
Fachhandel, KMU, Enterprise

DataCore Software bietet die branchenweit flexibelsten, intelligentesten und leistungsstärksten Software-Defined Storage-Lösungen für Block-, Datei - und Objektspeicher. Das Unternehmen unterstützt mehr als 10.000 Kunden weltweit bei der Speichermodernisierung, sowie dem Schutz und dem Zugriff auf ihre Daten. Mit einem umfassenden und auf eigenen Patenten basierenden Produktportfolio, sowie konkurrenzloser Erfahrung im Umfeld von Speicher Virtualisierung inklusive hochwertiger Datendienste ist DataCore das Maß der Dinge für Software-Defined Storage.

EUROSTOR

www.eurostor.com

Sitz der Gesellschaft:
Filderstadt

Jahr der Gründung:
2004

Zielgruppe:
gewerbliche Endkunden und Wiederverkäufer

EUROstor ist ein europaweit tätiger Hersteller von Speichersubsystemen, insbesondere RAID Systemen und Storage Appliances mit Sitz in Filderstadt (bei Stuttgart). Geschäftsführer von EUROstor ist Alexander Kraft. Für die technische Leitung verantwortlich ist Daniel Beuter. Wir entwickeln, fertigen und vertreiben europaweit hochwertige Datenspeichersysteme für den professionellen Einsatz und die spezifischen Anforderungen bei Unternehmen in der Großindustrie, dem Mittelstand sowie bei Forschung und Lehre. EUROstor vertreibt Produkte ausschließlich an gewerbliche Endkunden und Wiederverkäufer.

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.

Hitachi Vantara GmbH

www.hitachivantara.com

Sitz der Gesellschaft:
Tokyo

Niederlassungen in Deutschland:
Dreieich

Jahr der Gründung:
1910 (Hitachi)

Zielgruppe:
Großkunden, Mittelstand, KRITIS-Unternehmen, öffentliche Auftraggeber und Behörden sowie Systemhäuser

Hitachi Vantara verändert die Art und Weise, wie Daten Innovationen vorantreiben. Als hundertprozentige Tochtergesellschaft der Hitachi Ltd. bietet Hitachi Vantara die Datengrundlage, auf die sich Innovationsführer weltweit verlassen. Mit Datenspeicher, Infrastruktursystemen, Cloud-Management und digitaler Expertise hilft das Unternehmen seinen Kunden, die Grundlage für nachhaltiges Unternehmenswachstum zu schaffen.

US-Clouds und Grenzen der Datensouveränität im Rechenzentrum

DIGITALE SOUVERÄNITÄT IM STORAGE: WARUM STANDORT ALLEIN NICHT REICHT

US-Cloud-Anbieter werben mit »Sovereign Cloud« und europäischen Regionen, rechtlich bleiben Daten bei US-Konzernen jedoch im Zugriff ausländischer Behörden. Cloud-Act und FISA verschieben die Machtbalance deutlich zulasten europäischer Nutzer. Gefordert sind Architekturen, die Schlüsselhoheit, Rechtsraum und Kontrolle konsequent in europäische Hände legen.

Karl Fröhlich
speicherguide.de

Daten sind das Rückgrat der digitalen Wirtschaft – und ihre Sicherheit entscheidet über die Zukunftsfähigkeit deutscher Unternehmen. Doch während US-amerikanische Cloud-Anbieter mit »Sovereign Clouds« und EU-Konformität werben, bleibt eine zentrale Frage oft unbeantwortet: Wer kontrolliert die Unternehmensdaten wirklich? Trotz europäischer Rechenzentren und DSGVO-Siegeln sind Daten in US-Clouds niemals vor dem Zugriff amerikanischer Behörden geschützt. Der Grund: US-Gesetze wie der *US CLOUD Act* oder *FISA 702* hebeln nationale Regelungen aus – unabhängig vom physischen Speicherort. Für Unternehmen bedeutet das: Wahre Datensouveränität lässt sich nur mit Lösungen erreichen, die ausschließlich europäischer Rechtsprechung unterliegen. Wer Kontrolle und Vertrauen sichern will, braucht mehr als technische Versprechen – es geht um die strategische Unabhängigkeit und die Zukunft des eigenen Geschäfts.

Digitale Souveränität im Storage-Kontext

Digitale Souveränität im Storage-Kontext bedeutet die nachweisbare Fähigkeit eines Unternehmens, den gesamten Datenlebenszyklus unter eigenem Rechtsrahmen zu steuern. Gemeint sind technische und organisatorische Kontrolle über Zugriffe, Schlüsselmaterial, Betriebsprozesse und Exit-Szenarien. Entscheidend ist nicht der Ort allein, sondern wer effektiv Zugriff erzwingen oder verhindern kann. Souverän ist, wer Schlüsselgewalt besitzt, technische Durchsetzung betreibt, Betriebsautonomie organisiert, Portabilität sicherstellt und all das auditierbar belegt.

Abgrenzungen:

- Datensouveränität beschreibt die Entscheidungs- und Verfügungsrechte über Daten. Sie beantwortet das »Wer darf was« aus Sicht des Verantwortlichen, garantiert aber noch keine technische Durchsetzung.
- Cloud-Souveränität fokussiert auf die Nutzung von Cloud-Diensten unter Wahrung rechtlicher und operativer Kontrolle beim Kunden. Im Storage-Bereich heißt das Trennung von Daten- und Steuerungsebene, client-seitige Verschlüsselung mit kundenseitigen Schlüsseln sowie ein belastbarer Exit.
- Datenresidenz benennt Speicher- und Verarbeitungsstandorte. Sie ist notwendig, aber allein nicht ausreichend, da extraterritoriale Gesetze und Betriebswege weiterhin Zugriffe ermöglichen können.
- Datenhoheit wird häufig synonym zu Datensouveränität verwendet, legt den Schwerpunkt jedoch stärker auf den rechtlichen Anspruch als auf die operative Kontrolle.
- Compliance-Konformität belegt, dass Normen und Standards erfüllt sind. Sie ist ein Nachweis, aber kein Ersatz für echte Souveränität.
- Interoperabilität und Portabilität sind verwandte, aber unterschiedliche Ziele. Interoperabilität meint offene Protokolle und Formate, die Zusammenarbeit ermöglichen. Portabilität meint die praktikable Mitnahme von Daten und Metadaten zu anderen Anbietern innerhalb definierter Fristen.

Wachsender Handlungsdruck: US-Cloud-Gesetze werden zur Bedrohung

Der 2018 verabschiedete *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) stellt laut **Roland Stritt**, CRO bei **FAST LTA**, einen beispiellosen Bruch mit internationalen Rechtsnormen dar:

»Das Gesetz ermächtigt US-Strafverfolgungsbehörden, von amerikanischen Unternehmen die Herausgabe von Daten zu verlangen – unabhängig davon, wo diese Daten physisch gespeichert sind oder welche lokalen Gesetze deren Schutz vorsehen.«

Noch problematischer ist seiner Ansicht nach *Section 702* des *Foreign Intelligence Surveillance Act* (FISA 702), der ursprünglich für die Überwachung ausländischer Agenten konzipiert wurde, aber in der Praxis zur massenhaften Sammlung von Kommunikationsdaten aller Nicht-US-Bürger eingesetzt werden kann. »Im Gegensatz zum Cloud-Act, der zumindest formell richterliche Anordnungen erfordert, operiert FISA 702 weitgehend im Verborgenen«, warnt Stritt.

Das eigentliche Problem liegt aber nicht in der Existenz der US-Gesetze – die genannten Regularien bestehen bereits seit Jahren. Neu ist jedoch die geopolitische Lage: Die transatlantischen Beziehungen stehen unter verstärktem Druck, wirtschaftliche und politische Interessen driften zunehmend auseinander. Was früher als vertrauensvolle Partnerschaft galt, ist heute von Unsicherheiten und Rivalität geprägt.

Mit der US-Regierung hat sich mit ihrem Amtsantritt im Januar 2025 die öffentliche Wahrnehmung der USA in Deutschland in mehreren Punkten deutlich verändert – gerade in Bezug auf Vertrauen, Datenschutz und die Zusammenarbeit im Digitalbereich.

> » Wer die Souveränität an US-Konzerne abgibt, macht sich erpressbar und verliert die Kontrolle über das wertvollste Gut der Digitalwirtschaft: Daten. «
>
> **Roland Stritt, Fast LTA**

Foto: Fast LTA

Unter anderem wurden internationale Abkommen häufiger einseitig aufgekündigt oder infrage gestellt. Daher sehen deutsche Unternehmer die USA nicht mehr unbedingt als verlässlichen Partner. Laut *ARD-DeutschlandTREND* hielt im März nur noch jeder sechste Deutsche (16 Prozent) die USA für einen Partner, dem man vertrauen kann (-38 im Vgl. zu Oktober 2024).

Die Trump-Regierung hat die US-Interessen kompromisslos priorisiert und machte deutlich, dass wirtschaftliche und politische Vorteile für die USA stets Vorrang haben. Das hat Unternehmen und Politik in Deutschland sensibilisiert, dass amerikanische Partner im Zweifel nicht im gemeinsamen, sondern im eigenen Interesse handeln. Die politische Rhetorik wurde rauer, transatlantische Beziehungen kühler. Themen wie Wirtschaftssanktionen, Handelsstreitigkeiten und unterschiedliche Wertevorstellungen rückten stärker in den Vordergrund und verstärkten das Gefühl, künftig unabhängiger agieren zu müssen

Für deutsche Unternehmen bedeutet das: Vertrauliche Daten sind nicht mehr automatisch geschützt, nur weil sie »bei unseren amerikanischen Partnern« liegen. Im Gegenteil – in Zeiten wachsender wirtschaftlicher Spannungen kann der Zugriff auf zentrale Unternehmensdaten zum machtpolitischen Instrument werden. Wer jetzt nicht handelt, riskiert, die Kontrolle über das eigene digitale Kapital zu verlieren und sich erpressbar zu machen. Daher ist der Handlungsdruck für echte Datensouveränität heute größer denn je.

Risiko-Update durch KI, Regulierung und Geopolitik

Der neue Fokus ist allerdings nicht nur eine Frage von »Freund oder nicht«, sondern das Ergebnis eines Risiko-Updates auf mehreren Ebenen: Erstens verschieben KI- und Cloud-first-Strategien immer sensiblere Workloads in Managed-Umgebungen, wodurch Telemetrie, Metadaten und Modell-Trainingspfade neue Angriffs- und Ausleitungsflächen schaffen.

Zweitens steigen Haftung und Prüfungsdruck durch *NIS-2*, *DORA* und strengere Audits deutlich an, sodass bloße Standortzusagen nicht mehr genügen und eine nachweisbare Zugriffskontrolle verlangt wird. Drittens zeigen aktuelle Beschaffungsfälle und öffentliche Anhörungen, dass extraterritoriale US-Zugriffe nicht nur theoretisch sind, sondern in der Governance real berücksichtigt werden müssen.

Viertens verschärfen geopolitische Spannungen, Sanktionsregime und Lieferkettenrisiken die Abhängigkeit von Anbietern, die ausländischem Recht unterliegen. Kurz gesagt: Nicht

Praxischeck: Ist echte Souveränität gegeben

- Wer besitzt und verwaltet die produktiven Schlüssel, und kann der Anbieter Daten ohne diese Schlüssel lesen.
- Wo liegen KMS oder HSM operativ und rechtlich, und wie wird der Lebenszyklus der Schlüssel nachvollziehbar gesteuert.
- Wie werden Support-Zugriffe ausgelöst, genehmigt, protokolliert und wieder entzogen, und ist ein Zugriff ohne Kundenzustimmung technisch ausgeschlossen.
- Wie schnell und in welchen Formaten können Daten und Metadaten exportiert werden, und welche Fristen und Kosten sind vertraglich zugesichert.
- Sind WORM/Object-Lock und Retention-Bypass technisch verhindert und lückenlos auditierbar.

»Wir können uns nicht auf Unternehmen verlassen, die nicht unter unserer Jurisdiktion stehen.«

Peter Ganten, OSB Alliance

Foto: OSB Alliance

die Freundschaft hat sich geändert, sondern die Kombination aus Technologie, Regulierung, Transparenz und Geopolitik erhöht das Schadenspotenzial. Unternehmen müssen deshalb beweisbar kontrollieren können, wer wann worauf zugreift und unter welchem Rechtsrahmen dies geschieht.

Beispiele für die Abhängigkeit

Als die Diskussion zur digitalen Unabhängigkeit im Frühjahr so richtig an Fahrt aufnahm, gab es noch einige Gegenstimmen. Mittlerweile sind diese aber so gut wie verstummt, da es immer mehr negative Beispiele. Im Mai sperrte **Microsoft** das E-Mail-Konto des Chefanklägers am **Internationalen Strafgerichtshof** (IStGH), **Karim Khan**. Damit konnte der IStGH nur noch eingeschränkt bis gar nicht arbeiten. Laut einer Meldung der *Open Source Business Alliance* (OSBA) bildete eine *Executive Order* aus dem *Weißen Haus* die Grundlage für die Sanktionen gegen den IStGH und die dort beschäftigten Mitarbeitenden.

»Die von den USA angeordneten und von Microsoft mit umgesetzten Sanktionen gegen den internationalen Strafgerichtshof in Den Haag müssen ein Weckruf für alle sein, die für die sichere Verfügbarkeit staatlicher und privater IT- und Kommunikationsinfrastrukturen verantwortlich sind«, fordert **Peter Ganten**, Vorstandsvorsitzender der OSBA. »Sie zeigen: Wir können uns nicht auf Unternehmen verlassen, die nicht unter unserer Jurisdiktion stehen. Deswegen brauchen wir dringend Alternativen, die wir kontrollieren und gestalten können.«

Hinzukommt, dass die US-Regierung immer wieder Druck auf IT-Hersteller ausübt und zum Beispiel **Nvidia**-Verkäufe von AI-Chips nach China gestoppt hat. Mit Exportlizenzen und Zöllen wird zudem versucht Nicht-US-Firmen in der Lieferkette zu regulieren. Für die Befürchtung, die US-Regierung könnte Europa das Internet oder Cloud-Dienste abschalten, gibt es keine belastbaren Indizien. Den immer wieder zitierten »Kill-Switch« gibt es weder technisch, rechtlich noch gouvernance-seitig. Allerdings könnte Washington US-Unternehmen per Sanktionen, Exportkontrollen und Notstandsrecht (für US-Kommunikationsdienste im Inland) zu Geoblocking oder Service-Stopps gegenüber bestimmten Ländern/Organisationen zwingen. Der politische Hebel über US-Provider ist durchaus real. Daher macht es absolut Sinn, wenn europäische Unternehmen darüber nachdenken, Abhängigkeiten zu minimieren.

Was echte Datensouveränität für US-Anbieter tatsächlich bedeutet

US-Anbieter sprechen gern über »Souveränität«, adressieren aber oft nicht das Kernproblem. Es geht nicht um den physischen Speicherort allein, sondern um effektive Zugriffskontrolle unter kollidierenden Rechtsregimen. Solange US-Recht extraterritorische Zugriffspflichten kennt, reicht ein EU-Rechenzentrum mit EU-Support nicht aus, wenn Steuerungs-, Schlüssel- oder Betriebspfade weiterhin unter US-Herrschaft stehen. Damit Souveränität mehr ist als Verpackung, müssten US-Anbieter ihr Betriebs- und Geschäftsmodell in zentralen Punkten umbauen und wirtschaftliche sowie technische Zugeständnisse machen, die über Marketingbegriffe hinausgehen. Hier unser 5-Punkte-Plan:

1. Schlüsselhoheit beim Kunden und Client-seitige Verschlüsselung

Erstens braucht es eine Architektur, in der Kundendaten und Betriebsdaten strikt getrennt sind und in der US-Unternehmen keinen einseitigen Zugriff erzwingen können. Das verlangt Client-seitige Verschlüsselung mit kundenseitig kontrollierten Schlüsseln und optional HYOK-Modelle (Hold Your Own Key). BYOK (Bring Your Own Key) genügt nur, wenn der Schlüssel-Lebenszyklus vollständig außerhalb des Anbieterkontrollbereichs liegt. Der Control-Plane-Zugriff muss entkoppelt werden. Support darf nur just-in-time und genehmigungspflichtig über Customer-Lockbox-Mechanismen erfolgen. Telemetrie und Metadaten sind zu minimieren oder auf EU-Sichten zu beschränken, da sich aus Betriebsdaten Rückschlüsse auf Inhalte ziehen lassen.

2. Europäische Betriebsautonomie mit Treuhand- und Datentreuhänder-Modellen

Zweitens erfordert Glaubwürdigkeit eine rechtlich belastbare Organisationsstruktur in Europa. Gemeint ist nicht die übliche EU-Tochter, die letztlich der Mutter untersteht, sondern eine operative Eigenständigkeit mit europäischen Leitungsorganen, europäischer Schlüsselgewalt und vertraglich festgelegten Widerspruchs- und Anfechtungsprozessen bei Behördenanfragen. In kritischen Segmenten bieten sich Treuhand- und Datentreuhänder-Modelle an, bei denen ein europäischer Partner Betrieb und Zutrittsrechte verantwortet und der US-Anbieter nur Software liefert. Das verschiebt Haftung, Entscheidungswege und vor allem die tatsächliche Kontrolle.

3. Nachweisbare Transparenz durch unabhängige Audits und Offenlegung

Drittens braucht es überprüfbare

Transparenz statt Versprechen. Ohne unabhängige Audits der Souveränitätskontrollen, ohne veröffentlichte Richtlinien zum Umgang mit behördlichen Auskunftsersuchen und ohne statistische Transparenzberichte bleibt Souveränität Behauptung. Anbieter müssten offenlegen, wo sich Steuerungspunkte befinden, welche Subunternehmer eingebunden sind, wie Schlüsselmaterial gehandhabt wird und welche technischen Schranken selbst gegenüber dem eigenen Root-Personal gelten.

4. Produktstrategie unter Souveränitätsauflagen – Priorisieren, migrieren, exitfähig

Viertens sind Produktstrategie und Roadmaps anzupassen. Echte Souveränitätsfunktionen verursachen Reibung. Service-Parität zwischen globalem Angebot und souveräner Ausprägung wird vermutlich nicht immer zeitgleich möglich sein. Wer Souveränität ernst nimmt, priorisiert Workloads mit hohem Schutzbedarf, bietet klare Migrationspfade, definiert Exit-Szenarien mit nachweislicher Datenportabilität und akzeptiert, dass nicht jeder Managed-Komfort mit voller Souveränität vereinbar ist.

5. Ökonomische Konsequenzen realistisch einpreisen

Fünftens müssen ökonomische Konsequenzen adressiert werden. Souveräne Betriebsmodelle bedeuten zusätzliche Rechenzentrums-Segmente, restriktivere Telemetrie, komplexere Support-Prozesse und geringere Skaleneffekte. Das kostet Marge und bremst globale Vereinheitlichung. Solange US-Anbieter diesen Zielkonflikt nicht offen anerkennen und in ihre Preis- und Liefermodelle einpreisen, bleibt das Versprechen auf halbem Weg stehen.

Souveränität bedeutet kontrollierten Machtverzicht und EU-Governance

Kurz gesagt. Für US-Anbieter heißt Datensouveränität, Macht über Daten und Zugriffe freiwillig und überprüfbar abzugeben, technische Einblicke zu begrenzen, juristische Risiken zu schultern und europäische Governance nicht nur zu akzeptieren, sondern zu implementieren. Alles andere ist Regional-Branding.

An dieser Stelle gibt es natürlich auch den Ruf nach politischem Einschreiten. Mehr als Lippenbekenntnisse sind hier allerdings bisher nicht zu hören. Damit Europa unabhängiger von digitalen Importen aus dem Ausland wird, haben Deutschland und Frankreich den Gipfel für europäische digitale Souveränität in Berlin initiiert. Das darf durchaus als Signal gewertet werden.

Politische Signale und Hyperscaler-Investitionen

Wenn man allerding sieht, wie unreflektiert die Politik parteiübergreifend auf **Google**s Investitionsankündigung reagiert, scheint es mit dem Sachverstand nicht weit her zu sein. Der Hyperscaler will mit 5,5 Milliarden Euro den Ausbau von Rechenzentren und Infrastruktur in Deutschland vorantreiben.

Das klingt zunächst gut. Die Art und Weise, wie die Ankündigung politisch gefeiert wird, wertet Politikwissenschaftlerin **Frederike Kaltheuner** trotzdem als falsches Signal und erklärt im *tagesthemen*-Interview: »Dadurch wird nur der Status quo weiter zementiert. In der Souveränität geht es darum, die eigene Infrastruktur zu kontrollieren und wenn diese in ausländischer Hand ist, ist dies nicht der Fall.« Konkret sieht sie Gefahren in der nationalen Sicherheit und in Handelskonflikten. Bei transatlantischen Zerwürfnissen könne eine infrastrukturelle Abhängigkeit schnell zum »Gesprächsthema« werden.

Bisher wurde schlicht verschlafen, das Problem anzugehen. Daher brauche es jetzt Investitionen, Regulierung alleine reiche nicht. Man müsse den Markt öffnen, damit Innovationen und Alternativen erst entstehen können. Dabei sei wichtig, dass mit den Investitionen Alternativen geschaffen werden, weil der Versuch, die Amerikaner nachzubauen, nicht funktionieren werde.

Von den Investitionen der großen US-Tech-Konzerne wie zum Beispiel von Google fließt nur ein kleiner Teil tatsächlich nach Deutschland. Laut Kaltheuner schaffen Rechenzentren erstmal vor allem Jobs im Bau, diese sind aber temporär, und langfristig entstehen im Schnitt nur zwölf Arbeitsplätze pro Standort. Hinzu komme: Es werden derzeit RZs für sehr große KI-Modelle gebaut, und diese Infrastruktur ist so speziell, dass rund 70 Prozent der Investitionen wieder in die USA fließen. Denn auch Google müsse für diese Art von Rechenzentrum die Chips von Nvidia kaufen. Unter dem Strich stärkt das wirtschaftlich vor allem die US-Wirtschaft – nicht den Standort Deutschland.

Hier müssen Unternehmen erkennen, dass digitale Unabhängigkeit nichts ist, was die Politik mit der Gießkanne über alle verteilt. »Jede Investition in Unternehmen ist eine Entscheidung für oder gegen digitale Souveränität«, erklärt **Prof. Dr. Dennis-Kenji Kipker** vom **Cyberintelligence.Institute** in seiner S2N-Keynote in Regensburg. »Digitale Souveränität ist unsere eigene Aufgabe – das nimmt uns niemand ab.« ■

> »Digitale Souveränität ist unsere eigene Aufgabe – das nimmt uns niemand ab.«
>
> **Dennis-Kenji Kipker, Cyberintelligence.Institute**

Bild: Dennis-Kenji Kipker

NIS-2: Was Rechenzentren jetzt konkret umsetzen müssen

GESETZLICH VERORDNETE CYBERSICHERHEITSPFLICHTEN

Karl Fröhlich
speicherguide.de

Mit dem NIS-2-Umsetzungsgesetz hat der Bundestag den Rechtsrahmen für Cybersicherheit beschlossen. Eine allgemeine Übergangsfrist gibt es nicht, zugleich wächst der Kreis betroffener Unternehmen deutlich. Geschäftsleitungen und IT-Abteilungen müssen Governance, Technik und Prozesse nun zügig auf NIS-2-Niveau bringen.

Mit dem Beschluss des *NIS-2*-Umsetzungsgesetzes am 13. November 2025 ist der politische Teil der NIS-2-Umsetzung in Deutschland abgeschlossen. Das neue *BSIG-neu* wird nach Befassung im Bundesrat und Verkündung im Bundesgesetzblatt in Kraft treten und macht die europäischen Vorgaben zur Cybersicherheit für Unternehmen verbindlich. Eine generelle Schonfrist ist nicht vorgesehen: Die materiellen Pflichten gelten im Grundsatz ab Inkrafttreten, Nachweise können im Regelfall frühestens drei Jahre später verlangt werden. Betroffene Einrichtungen müssen sich innerhalb von drei Monaten nach Einstufung beim **BSI** (Bundesamt für Sicherheit in der Informationstechnik) registrieren.

»Die Umsetzung der europäischen NIS-2-Richtlinie war überfällig«, sagt **Bitkom**-Präsident **Dr. Ralf Wintergerst**. »Cyberangriffe bedrohen Wirtschaft, Verwaltung und Gesellschaft. Den deutschen Unternehmen ist so zuletzt ein jährlicher Schaden von 202 Milliarden Euro entstanden. Ziel der NIS-2-Richtlinie ist die Stärkung von Resilienz und Cybersicherheit in den Mitgliedstaaten. Dafür wurde unter anderem die Definition kritischer Infrastruktur erweitert und damit eine Vielzahl von Unternehmen zu besonderen Sicherheitsvorkehrungen verpflichtet.«

Geschäftsleitung steht in der Pflicht

NIS-2 weitet den Anwendungsbereich deutlich aus. Neben kritischen Infrastrukturen werden künftig zehntausende »wesentliche« und »wichtige« Einrichtungen erfasst, darunter mittlere Unternehmen ab 50 Mitarbeitenden oder mehr als zehn Millionen Euro Umsatz bzw. 43 Millionen Euro Bilanzsumme in sicherheitsrelevanten Sektoren. Rechenzentrums-Betreiber, Managed-Service-Provider und IT-Dienstleister geraten damit noch stärker in den Fokus – sowohl als unmittelbar betroffene Einrichtungen als auch über die Lieferketten-Anforderungen ihrer Großkunden.

Kern der Vorgaben ist ein risikobasiertes Informationssicherheits-Management mit klaren Verantwortlichkeiten. Die Geschäftsleitung bleibt in der Pflicht und kann sich nicht auf eine rein formale Delegation an die IT-Abteilung zurückziehen. Gefordert sind angemessene technische und organisatorische Maßnahmen, ein strukturiertes Schwachstellen- und Vorfall-Management sowie ein dreistufiges Melderegime bei Sicherheitsvorfällen mit engen Fristen. Verstöße können mit hohen Bußgeldern und persönlicher Haftung der Leitungsorgane geahndet werden.

Hohe Cybersicherheitsstandards – aber Kritik an Verbotsrecht

Positiv bewertet der Bitkom, dass im nun verabschiedeten Gesetz nachgelagerte Bundesbehörden in den Anwendungsbereich von NIS-2 einbezogen werden. Besonders in sensiblen Bereichen der Bundesverwaltung können Sicherheitslücken erhebliche finanzielle Schäden verursachen und das Vertrauen in demokratische Institutionen beschädigen. »Eine wirksame und glaubwürdige Cybersicherheitsarchitektur setzt voraus, dass der Staat selbst höchste Sicherheitsstandards einhält«, mahnt Wintergerst. »Es ist nur konsequent und richtig, dass Bundesbehörden künftig denselben Anforderungen beim Risikomanagement unterliegen wie regulierte Unternehmen.«

Dagegen sind die zuletzt in das Gesetzgebungsverfahren eingebrachten Neuregelungen zu sogenannten kritischen Komponenten nach Ansicht des Bitkom eher schädlich. Vorgesehen ist nun, dass das Bundesinnenministerium in Abstimmung mit anderen Ressorts kritische Komponenten definiert und künftig auch eigenständig deren Einsatz untersagen kann. »Unternehmen brauchen verlässliche Rahmenbedingungen, Verbote können erhebliche Auswirkungen auf die Geschäftstätigkeit haben«, erklärt Wintergerst. »Vor solch wichtigen Entscheidungen müssen die Betroffenen unbedingt vorab konsultiert werden.« Die Definition von kritischen Komponenten sollte nach Ansicht des Bitkom auch künftig auf Grundlage technischer Kriterien durch die Bundesnetzagentur und das BSI erfolgen.

Datensicherung an den Stand der Technik anpassen

Für Rechenzentren und IT-Abteilungen spielt Datensicherung eine Schlüsselrolle. Backup- und Disaster-Recovery-Konzepte sollten an den Stand der Technik angepasst werden. Dazu zählen etwa der Einsatz unveränderbarer Speichertechnologien, eine nachweisbare 3-2-1-1-Backup-Strategie, regelmäßige Wiederherstellungstests und ein integriertes Monitoring der Backup-Infrastruktur. Auch SaaS-Umgebungen und Identitätsdienste müssen in diese Betrachtung einbezogen werden, um Geschäftsprozesse im Ernstfall tatsächlich wiederherstellen zu können. Viele Unternehmen sind laut Umfragen noch nicht ausreichend vorbereitet. Angesichts fehlender Übergangsfrist und wachsender Prüf- und Nachweispflichten empfiehlt sich ein strukturiertes Vorgehen, das Ressourcen schont und gleichzeitig regulatorische Risiken reduziert.

Handlungshinweise für Rechenzentren und IT-Abteilungen

- **Betroffenheit klären:** Einstufung als wesentliche/wichtige Einrichtung prüfen und Scope (Rechenzentren, Services, Mandanten, Lieferkette) sauber abgrenzen.
- **Governance festziehen:** Verantwortlichkeiten für Informationssicherheit, Incident-Handling und Reporting definieren, Management einbinden und Berichtsroutinen etablieren.
- **Risikobild schärfen:** Bestehendes ISMS, Backup-Strategie, Netzwerk-Segmentierung und Monitoring gegen NIS-2-Anforderungen spiegeln, Lücken dokumentieren und priorisieren.
- **Melde- und Registrierungsprozesse einrichten:** Registrierung beim BSI vorbereiten, interne Meldeketten für Vorfälle mit 24/72-Stunden-Fristen definieren und in Notfallpläne integrieren.
- **Lieferketten absichern:** Verträge mit Hosting-, Cloud- und Security-Providern sowie Software-Lieferanten auf NIS-2-Tauglichkeit prüfen und Sicherheitsanforderungen vertraglich verankern. ■

Fachhändler für Storage-Systeme

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
Kastanienallee 22, 14052 Berlin
Tel. 030/308 83 80, Fax 030/30 88 38 30
E-mail: 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 + Softwarelösungen SE
Leverkusenstraße 54, 22761 Hamburg
Tel. 040/51 12 10, Fax 040/51 12 11 11
info@comline-se.de, www.comline-se.de

eSell Nord GmbH
Rotdorntwiete 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 & Netzwerksysteme 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

Convotis GmbH
Neuer Zollhof 3, 40221 Düsseldorf
info@convotis.com, Tel. 0211/54 57 21-700
www.convotis.com

Cancom GmbH
Elisabeth-Selbert-Str. 4a, 40764 Langenfeld
Tel. 02173/5966 0, www.cancom.de

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

i-Tech GmbH & Co. KG
Campus Fichtenhain 42, 47807 Krefeld
Tel. 021 51/579 95 80, Fax 021 51/57 99 58 58
info@i-tech24.de, www.i-tech24.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
Hafenstrasse 11, 49090 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

Silent Brick System: Modulare Storage-Architektur für moderne Datensicherungen

AIR-GAP, UNVERÄNDERLICHKEIT UND EU-DATENSOUVERÄNITÄT FÜR BACKUPS

Backup-Infrastrukturen stehen vor neuen Anforderungen: Datenmengen wachsen rasant, zugleich müssen Systeme vor Ransomware geschützt, Compliance-Anforderungen erfüllt und Kapazitäten flexibel skalierbar bleiben – bei voller Kontrolle über sensible Daten. Das Silent Brick System von FAST LTA setzt dafür auf einen bewusst von klassischen Storage-Architekturen abweichenden Ansatz.

Hannes Heckel
FAST LTA

Das zentrale Designprinzip des *Silent Brick Systems* von **FAST LTA** ist die konsequente Trennung von Controller und Speichermedien. Anders als monolithische Storage-Arrays ermöglicht diese Architektur, Controller und Datenträger unabhängig voneinander zu aktualisieren, auszutauschen oder zu erweitern. Speichermedien lassen sich ohne Datenmigration zwischen verschiedenen Controllern bewegen, technologische Innovationen nahtlos integrieren – eine Investitionssicherheit, die in der Storage-Branche selten ist.

Das Herzstück bildet der *Controller X*, verfügbar in drei Ausbaustufen mit zwei, vier oder acht Slots. Er nimmt NVMe-basierte *Silent Brick Pro*-Module auf und bietet bis zu 768 TByte Bruttokapazität an NVMe-Storage auf zwei Höheneinheiten. Die Top-Konfiguration *X6080* mit 100-Gbit-Ethernet erreicht konstante Datenübertragungsraten von bis zu 6 GByte/s. Für Kapazitätserweiterungen lassen sich zusätzlich bis zu 26 *Silent Brick Max*-Einheiten über SAS anbinden – die Gesamtkapazität skaliert damit auf über 6 PByte.

Drei Speichermedien für unterschiedliche Anforderungsprofile

Die Flexibilität des Systems zeigt sich in der Medienauswahl. Silent Brick Pro ist für Performance-Szenarien konzipiert: Jeder Brick enthält zwölf M.2-NVMe-Module aus drei verschiedenen Produktionschargen und erreicht bis zu 96 TByte Bruttokapazität bei 520 Gramm Gewicht. Das robuste Aluminiumgehäuse in Taschenbuchgröße macht die Module nicht nur transportabel, sondern ermöglicht echtes Air-Gap – sie können physisch vom System getrennt, sicher verwahrt oder im Safe gelagert werden. Die Übertragungsraten prädestinieren die Pro-Variante für tägliche inkrementelle Backups und Instant Recovery: Virtuelle Maschinen starten direkt vom Backup, noch während die vollständige Wiederherstellung läuft.

Silent Brick Max adressiert Kapazitätsanforderungen im Secondary Target. Diese stationären 19-Zoll-Module packen bis zu 240 TByte auf eine Höheneinheit und enthalten ebenfalls zwölf Festplatten aus drei verschiedenen Chargen – ein bewährtes Redundanzprinzip zur Vermeidung korrelierter Ausfälle.

Ab 2026 ergänzt *Silent Brick Max Air* das Portfolio als erste nicht entnehmbare Storage-Einheit mit zwei echten Air-Gap-Modi. Im »Manual«-Modus lässt sich der Air-Gap ausschließlich über einen physischen Taster am Gerät aufheben. Der innovative »Timer«-Modus hebt die Isolation nach einem vordefinierten Intervall automatisch auf – eine Kombination aus echter Air-Gap-Sicherheit und operativer Flexibilität.

Mehrschichtige Datensicherheit

Die Sicherheitsarchitektur basiert auf mehreren Ebenen. Jedes Speichermodul verkraftet den gleichzeitigen Ausfall von bis zu vier Datenträgern ohne Datenverlust. Diese Resilienz erreicht FAST LTA durch Erasure-Coding mit vierfacher Redundanz – eine der RAID-Technologie überlegene Methode. Ver-

Bild: FAST LTA

Das Silent Brick System kombiniert NVMe-Performance, HDD-Wirtschaftlichkeit, hohe Skalierbarkeit und echten Air-Gap.

Bestückt mit zwölf HDDs im 3,5-Zoll-Format bietet der Silent Brick Max (Air) die beste Balance zwischen hoher Kapazität und niedrigen Speicherkosten.

stärkt wird dies durch den systematischen Einsatz verschiedener Festplattenchargen: Jedes Modul enthält vier Laufwerke aus drei unterschiedlichen Produktionsserien, um korrelierte Ausfälle durch Serienfehler zu verhindern.

Eine zusätzliche Schutzebene bietet der Digital Audit. Diese permanente Selbstüberwachung prüft die gespeicherten Daten automatisch bitgenau, erkennt Fehlfunktionen frühzeitig und korrigiert sie. Zusammen mit Immutability-Funktionen – kontinuierliche Snapshots, S3 Object Locking oder physischer Air-Gap – entsteht ein umfassendes Schutzsystem gegen Ransomware-Angriffe.

Flexible Betriebsmodi für verschiedene Einsatzszenarien

Das Silent Brick System unterstützt verschiedene Betriebsmodi. Als SecureNAS mit ZFS-Dateisystem und Triple-Parity lässt es sich über NFS- oder SMB-Shares einbinden und parallel über S3-kompatible Protokolle ansprechen. Im VTL-Modus (Virtual Tape Library) wird es direkt von der Backup-Software gesteuert und kann Medien »auswerfen« – ein echter Air Gap ohne Bandtechnologie. Als VTL-Archiv skaliert das System problemlos in den Petabyte-Bereich.

Die Integration mit gängigen Backup-Lösungen ist nahtlos. Silent Bricks sind als »Veeam Ready« zertifiziert und unterstützen Funktionen wie *Instant VM Recovery*, *SureBackup* und die S3-basierte *Object Storage API* mit Immutability.

Unterschiedliche Backup-Strategien lassen sich flexibel umsetzen: Performance-Bereiche für Primary-Targets mit Silent Brick Pro und kurzen RTOs, Kapazitätsbereiche mit Silent Brick Max als Secondary-Target, Air-Gap-Bereiche durch entnehmbare Silent Brick Pro oder stationäre Silent Brick Max Air. Diese unabhängige Skalierbarkeit der einzelnen Speicherbereiche gehört zu den Kernstärken des Systems.

EU-Datensouveränität als Differenzierungsmerkmal

In Zeiten zunehmender Fokussierung auf Datenschutz und digitale Souveränität gewinnt die Herkunft von Storage-Systemen an Bedeutung. FAST LTA entwickelt, fertigt und wartet seine Produkte in Deutschland. Diese vollständige Lokalisierung in der EU bedeutet nicht nur kurze Wege für Service und Support, sondern auch Schutz vor extraterritorialen Zugriffsrechten wie dem *US CLOUD Act*. Für Organisationen, die personenbezogene oder hochsensible Daten verarbeiten, ist dies ein entscheidender Faktor: Die Systeme erfüllen die Anforderungen der *EU-DSGVO* von Grund auf und gewährleisten, dass Daten die europäische Rechtshoheit nicht verlassen.

Diese Datensouveränität erstreckt sich auf die gesamte Lieferkette: FAST LTA setzt auf EU-Partner und vermeidet Abhängigkeiten von Anbietern unter US-Gesetzgebung. Während Cloud-Anbieter mit »Sovereign Clouds« werben, deren Infrastrukturen dennoch unter amerikanischem Recht stehen, bietet ein vollständig in der EU entwickeltes und produziertes System eine verlässliche Alternative.

Präzise Abstimmung auf individuelle Anforderungen

Moderne Backup-Infrastrukturen müssen unterschiedliche, teils widersprüchliche Anforderungen in Einklang bringen: Performance und Kapazität, Kosten und Sicherheit, Flexibilität und Standardisierung. Das Silent Brick System adressiert diese Herausforderung durch seinen modularen Ansatz. Performance-kritische Bereiche erhalten NVMe-Medien, kostenoptimierte Bereiche setzen auf HDD-basierte Speichereinheiten, Air-Gap-Bereiche nutzen entnehmbare oder automatisch isolierte Medien.

Das Ergebnis ist eine Storage-Architektur, die sich organisch mit den Anforderungen entwickelt. Neue Medien lassen sich hinzufügen, ohne bestehende Konfigurationen zu beeinträchtigen. Technologische Sprünge – etwa von HDD zu NVMe – werden durch den modularen Aufbau absorbiert, ohne das Gesamtsystem zu entwerten. Die physische Trennung von Controller und Medium ermöglicht es, Daten dort zu lagern, wo sie aus Sicherheits-, Compliance- oder Kostengesichtspunkten hingehören – im Rack, im Safe oder an einem zweiten Standort.

Ein anderer Weg in der Storage-Architektur

Das Silent Brick System entzieht sich bewusst den Konventionen traditioneller Storage-Arrays. Es ist weder ein reines NAS noch eine klassische VTL, weder ein Object Store noch ein Tape-Ersatz – kann aber all diese Rollen übernehmen. Diese Vielseitigkeit entspringt einer Architektur, die Speichermedien nicht als fest verbaute Komponenten begreift, sondern als eigenständige, flexible Bausteine einer Gesamtstrategie.

Für Organisationen, die ihre Datensicherung auf eine Grundlage stellen wollen, die technologische Weiterentwicklung und regulatorische Anforderungen gleichermaßen berücksichtigt, bietet dieser Ansatz einen alternativen Weg. Das Silent Brick System zeigt, dass umfassende Sicherheit und operative Flexibilität kein Widerspruch sein müssen – wenn man bereit ist, Storage-Architekturen grundlegend neu zu denken. ■

Weitere Informationen:

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

»8 Nines«-Verfügbarkeit mit 50 Mio. IOPS & FIPS 140-3 Level 2-Zertifizierung

ENTERPRISE-STORAGE FÜR KI-WORKLOADS

KI-Workloads und verteilte Daten bringen klassische Storage-Architekturen an Grenzen. Hitachis All-Flash-System VSP One Block High End liefert bis zu 50 Mio. IOPS, 8x9 Verfügbarkeit, FIPS-140-3-Zertifizierung sowie Cyber-Resilienz- und Data-Reduction-Garantien – verwaltet über die Unified-Management-Plattform VSP 360.

Frank Hörner
Hitachi Vantara

AI-Workloads, Real-Time-Analytics und exponentielles Datenwachstum überfordern klassische Storage-Architekturen. Über 70 Prozent der Unternehmen halten ihre IT-Infrastruktur für unzureichend vorbereitet auf ML- und KI-Anforderungen (Quelle: *S&P Global*), während gleichzeitig 57 Prozent der IT-Leiter Daten über On-Premises-, Private-, Hybrid- und Public-Cloud-Umgebungen verteilen (Quelle: Hitachi Studie »State of Data Infrastructure Global Report 2024«).

Mit der *VSP One Block High End* bringt **Hitachi Vantara** Anfang 2026 ein All-Flash NVMe Block Storage System auf den Markt, das diese Herausforderungen adressiert.

Technische Eckdaten

Das System basiert auf einer All-Flash-NVMe-Architektur und liefert bis zu 50 Millionen IOPS mit Hardware-Compression-Beschleunigung und einer Dichte von bis zu 120 TByte pro Rack Unit. Die Skalierung erreicht bei voller Ausbaustufe 12 Controller und maximal 288 x 60 TByte SSDs mit einer Latenz von 37 Mikrosekunden und einem Durchsatz von bis zu 633 GByte/s.

Connectivity umfasst 100G NVMe over TCP und 64G Fibre Channel mit bis zu 192 Host Ports. Die adaptive Datenkompression hält die Performance auch bei unkomprimierbaren Daten aufrecht. Besonders relevant für regulierte Branchen: VSP One Block High End ist *FIPS 140-3 Level 2* zertifiziert und erfüllt das Secure Software Development Framework der US-Regierung – validiert durch CISA.

Die Verfügbarkeit wird mit acht Nines (99,999999 Prozent) angegeben – das entspricht 0,315 Sekunden Downtime pro Jahr, weniger als ein Administrator braucht, um »Ausfall« zu sagen. Abgesichert durch Hitachis 100-prozentige Data Availability Guarantee, die das Unternehmen seit über 20 Jahren anbietet.

Foto: Hitachi

Cyber Resilience als Kaufargument

Ransomware-Attacken haben Storage-Anforderungen verändert. Die VSP One liefert immutable Snapshots, automatisierte Recovery-Prozesse und Anomalie-Erkennung durch *Cyber-Sense*. Die *Cyber Resilience Guarantee* verspricht Clean-Data-Recovery in Sekunden nach Ransomware-Angriffen. Die *4:1 Data Reduction Guarantee* sorgt für kalkulierbare Speichereffizienz bei gleichbleibender Performance.

VSP One: Das letzte Puzzle-Teil

Mit der VSP One Block High End komplettiert Hitachi Vantara sein VSP One Block-Portfolio. Während Midrange-Block-Storage, File, Object und Software-Defined Storage bereits verfügbar waren, kommt jetzt die High-End-Appliance für mission-critical Workloads hinzu. Vom Midrange-Einstieg bis zur Hochleistungsplattform für AI-Factories – alle Komponenten unter einer einheitlichen Management-Plattform.

Das bedeutet konkret: Unternehmen können ihre gesamte Storage-Infrastruktur standardisieren, unabhängig davon, ob es um Dateiserver, Object

Storage für Backups, Software-Defined Storage am Edge oder eben mission-critical Datenbanken geht. Alles läuft unter der einheitlichen Management-Oberfläche *VSP 360*.

Diese Architektur ermöglicht echte Workload-Konsolidierung: Open-Systems-Workloads (Block, File, Object) und Mainframe-Umgebungen laufen auf einer einheitlichen Plattform. Für Unternehmen mit historisch gewachsenen, heterogenen IT-Landschaften bedeutet das messbar weniger Management-Overhead.

Für echte Hybrid-Cloud-Strategien ist die VSP One Block High End die On-Premises-Komponente. Die Cloud-Seite liefert die VSP One SDS (Software-defined Storage), die auf *Microsoft Azure*, *AWS* und *Google Cloud* läuft. Bidirektionale asynchrone Replikation zwischen On-Premises und Cloud ermöglicht flexible Disaster-Recovery-Strategien, Cloud-Bursting für AI-Training-Umgebungen und nahtlose Workload-Mobilität – alles zentral über VSP 360 verwaltet.

Ein weiterer Vorteil: Die VSP One Block High End kann bestehende Storage-Systeme, auch von Drittherstellern, virtualisieren. Legacy-Kapazitäten lassen sich einbinden und über VSP 360 verwalten, als wären sie Teil der Hitachi-Infrastruktur. Kunden müssen vorhandene Speicherkapazität nicht neu kaufen, sondern können sie weiterverwenden.

VSP 360: Unified Management als Differenzierungsmerkmal

Der zentrale Unterschied zu fragmentierten Multi-Vendor-Umgebungen liegt in VSP 360, der übergreifenden Management-Plattform, die auf drei Säulen basiert:

Control: Fleet-Management über Block, File, Object und Software-defined Storage hinweg. Hybrid-Cloud-Orchestrierung aus einer Konsole, ohne Applikationen neu zu schreiben oder Tools zu wechseln. Deployment und Verwaltung über On-Premises und Cloud-Umgebungen hinweg.

Ein oft unterschätzter Vorteil: Alle VSP One Systeme nutzen das gleiche

Foto: Hitachi

Betriebssystem (*SVOS RF*). Administratoren, die mit einem *VSP Block 24 Midrange*-System arbeiten, kennen automatisch auch die VSP One Block High End – keine Lernkurve, keine unterschiedlichen Interfaces. Viele Wettbewerber kämpfen mit fragmentierten Portfolios aus zugekauften Technologien und entsprechend unterschiedlichen Management-Oberflächen.

Observe: AIOps-gestützte Analytics liefern prädiktive Insights zu Performance, Kapazität, Security und System-Health. Zugänglich via SaaS, Mobile oder On-Premises.

Govern: Policy-Enforcement, Compliance und Lifecycle-Management für Hybrid-Umgebungen. Unterstützt AI-Workloads, Cybersecurity und PII-Klassifizierung mit präziser Kontrolle über Datenlokationen.

Für IT-Teams mit begrenzten Ressourcen bedeutet das: Ein Interface statt fünf verschiedener Management-Tools. Automatisierte Workflows statt manueller Storage-Provisionierung. Zentrale Governance statt fragmentierter Policies.

Datensouveränität und Compliance

Die VSP One Block High End operiert vollständig On-Premises. In Zeiten von *CLOUD Act* versus *DSGVO*-Konflikten ist das für regulierte Branchen, von Finanzdienstleistungen über Gesundheitswesen bis zu kritischen Infrastrukturen, ein handfestes Kaufargument. VSP 360 ermöglicht präzise Kontrolle über Datenlokationen, wichtig für DSGVO, kommende *EU Data Act*-Anforderungen und branchenspezifische Regulierungen. FIPS 140-3 Level 2 und CISA-Validierung sind in öffentlichen Ausschreibungen oft Pflichtkriterien.

Nachhaltigkeit durch Design

Die VSP One schaltet CPUs automatisch in einen Eco-Modus bei niedriger Aktivität, was Energieverbrauch und CO_2-Fußabdruck reduziert. Die Systeme sind *EnergyStar*-zertifiziert und liefern branchenweit die höchsten IOPS pro Watt. In Kombination mit der 4:1 Data Reduction Guarantee lassen sich Rechenzentrumsressourcen effizienter nutzen, ein zunehmend wichtiges Kaufkriterium, auch vor dem Hintergrund steigender Energiekosten und verschärfter ESG-Berichtspflichten.

Zuverlässigkeit als Innovationstreiber

IT-Teams mit hochverfügbarer Storage-Infrastruktur verbringen weniger Zeit mit Firefighting und mehr mit wertschöpfenden Projekten. Acht Nines Verfügbarkeit, automatisierte Recovery und garantierte Performance schaffen Freiraum für AI-Initiativen und digitale Transformation statt reaktivem Troubleshooting. In Zeiten des Fachkräftemangels ist das ein handfestes Kaufargument: weniger Betriebsaufwand bei höherer Zuverlässigkeit.

Verfügbarkeit und Partner

Die VSP One Block High End wird Anfang 2026 global über Hitachi Vantara und dessen Partnernetzwerk verfügbar sein. ■

Weitere Informationen:

Hitachi Vantara
Im Steingrund 10
63303 Dreieich
Tel. 06103 8040
www.hitachivantara.com/de-de/

Speicherstrategie: Manipulationssichere Daten mit WORM & Selbstheilung

CYBER-RESILIENZ IM MITTELSTAND

Ransomware, Datenwachstum und Compliance zwingen KMU über klassisches Backup hinauszudenken: Moderne Speicherplattformen wie DataCore Swarm und die rapidSWARM SNS Appliance von N-Tec schützen Daten zuverlässig vor Manipulation, Ausfällen und Ransomware – einfach integrierbar, skalierbar und wirtschaftlich.

Sven Meyerhofer
N-Tec

Die digitale Transformation eröffnet mittelständischen Unternehmen neue Möglichkeiten – verstärkt aber auch die Abhängigkeit von leistungsfähigen, sicheren und ausfallsicheren IT-Infrastrukturen. Herkömmliche Backup-Strategien geraten dabei zunehmend an ihre Leistungsgrenzen. Spätestens wenn Ransomware-Attacken, Hardware-Ausfälle oder verschärfte regulatorische Vorgaben eintreten, zeigt sich die wahre Belastbarkeit der Speichersysteme.

Traditionelle Backups sichern zwar gegen Datenverlust ab, bieten jedoch keinen Schutz vor gezielter Manipulation, Verschlüsselung durch Angreifer oder dem Verlust der Datenintegrität. Hinzu kommen exponentiell wachsende Datenvolumina, verschärfte rechtliche Rahmenbedingungen und dezentrale IT-Landschaften, die eine durchgängige Datensicherung zusätzlich erschweren.

Cyber-Resilienz statt klassischer Datensicherung

Mittelständische Betriebe stehen daher vor der Aufgabe, ihre Daten nicht nur zu speichern, sondern langfristig manipulationssicher, hochverfügbar und revisionsfest vorzuhalten. Der Begriff Cyber-Resilienz beschreibt diese erweiterte Anforderung präzise: IT-Systeme müssen Angriffe oder Störfälle nicht nur bewältigen, sondern auch zeitnah und kontrolliert wiederherstellbar sein – ohne dass Geschäftsprozesse länger unterbrochen werden.

In diesem Kontext gewinnen moderne Speicherplattformen mit softwaredefinierter Architektur, feingranularer Zugriffskontrolle, Verschlüsselung und automatischen Reparaturmechanismen zunehmend an Relevanz. Sie bilden das Fundament, um geschäftskritische Daten zuverlässig vor Verlust oder Veränderung zu schützen und gleichzeitig regulatorische Anforderungen zu erfüllen.

Genau hier setzen die gemeinsamen Lösungen von **DataCore** und **N-Tec** an, die eine hochintegrierte, praxistaugliche Speicherarchitektur für den Mittelstand bereitstellen.

DataCore Swarm – Fundament moderner Datensouveränität

Mit *Swarm* stellt DataCore eine ausgereifte On-Prem-Objektspeicher-Plattform bereit, die Datenspeicherung, Schutz und Administration in einer einheitlichen, softwaredefinierten Architektur bündelt. Der *DataCore Single Node Swarm* ist die kompakte Ausführung, speziell entwickelt für dezentrale oder Edge-Szenarien in mittelständischen Unternehmen, in denen Daten unmittelbar am Entstehungsort erfasst und gesichert werden müssen.

Technologisch basiert Single Node Swarm auf einer containerisierten Architektur, die vollständig auf *Kubernetes* aufbaut. Dies ermöglicht eine flexible Bereitstellung, Skalierung und Verwaltung von Speicher-Ressourcen – unabhängig von der eingesetzten Hardware. Eine intuitive, webbasierte Administrationsoberfläche gibt IT-Ver-

Grafik: DataCore

Alle Eigenschaften von rapidSwarm SNS.

antwortlichen zentrale Kontrolle über alle Speicher- und Zugriffsprozesse.

Aktives Archiv: WORM, Verschlüsselung, Selbstheilung

Besonders bemerkenswert ist die konsequente Implementierung von Datensicherheit und Integrität. Die WORM-Funktionalität (»Write Once, Read Many«) stellt sicher, dass gespeicherte Daten weder modifiziert noch gelöscht werden können – ein zentrales Merkmal für revisionssichere Archivierung und Ransomware-Schutz. Ergänzend werden sämtliche Daten sowohl im Ruhezustand als auch während der Übertragung verschlüsselt, während Hashing-Verfahren und Aktivitätsprotokolle für vollständige Nachvollziehbarkeit sorgen.

Effizienz durch Automatisierung und Datei-Tiering

Darüber hinaus bietet Swarm aktiven Schutz vor physischen Fehlerquellen wie Bit-Rot und Laufwerksausfällen. Selbstheilungsmechanismen identifizieren beschädigte Segmente automatisch und rekonstruieren sie ohne manuellen Eingriff. Der bewusste Verzicht auf ein konventionelles Dateisystem reduziert zudem die Angriffsfläche – ein strategischer Vorteil im Kampf gegen Malware und Social Engineering.

Ein weiterer zentraler Vorteil liegt in der Fähigkeit, aktive Archive direkt am Datenursprung zu etablieren. Swarm ermöglicht die Langzeitspeicherung von Daten bei gleichzeitiger permanenter Verfügbarkeit. Die integrierte Metadatenverwaltung unterstützt gezielte Such- und Wiederherstellungsvorgänge, einschließlich selektiver Teilwiederherstellung und Streaming umfangreicher Dateien.

rapidSWARM SNS Appliance, die schlüsselfertige All-in-one"
Objekt Speicher Lösung

rapidSWARM SNS	S	M	L
Nutzbare Kapazität	25+ TB	50+ TB	100+ TB
CPU	2 x 16Core (Gen4)		
RAM	256GB	256GB	512GB
Boot + Elastic Search (Cache)	2 x 2TB NVMe M2		
Datenplatten	8 x 8TB NLSAS	8 x 16TB NL SAS	8 x 24 TB NLSAS
Netzwerk	2x GbE + 2x 10/25GBit + IPMI		
Appliance	red. PSU und Lüfter, max Leistungsaufnahme 520W, Temp: 0°C bis ~ 40°C, Rackmount 2 HE, T 673mm, 34KG (inkl. 8x HDD)		

Grafik: DataCore

N-Tec rapidSWARM SNS – schlüsselfertige Appliance vorkonfiguriert in den Größen S, M und L.

Sicherheit durch Architektur

Für vorhandene Infrastrukturen bietet DataCore mit *FileFly* ein regelbasiertes Datei-Tiering, das selten genutzte Dateien automatisch von kostenintensiven NAS-Systemen auf kostengünstigen Objektspeicher migriert – ohne Betriebsunterbrechung. Dies senkt nicht nur die Speicherkosten erheblich, sondern verkürzt auch Backup- und Restore-Zeiten merklich.

Mit dieser Kombination aus Leistung, Automatisierung und Sicherheit bildet DataCore Swarm die technologische Grundlage für resiliente Datenspeicherung – eine optimale Lösung für Unternehmen mit hohen Anforderungen an Datenschutz, Verfügbarkeit und Compliance, die jedoch keine komplexe Großrechnerinfrastruktur betreiben möchten.

N-Tec rapidSWARM SNS – praxisgerechte Umsetzung für den Mittelstand

Während DataCore die technologische Plattform liefert, übernimmt N-Tec als erfahrener Systemintegrator und Hersteller maßgeschneiderter Storage-Appliances die praxisgerechte Umsetzung für mittelständische Anforderungen. Mit *rapidSWARM SNS* bietet N-Tec eine betriebsfertige, vollständig integrierte Appliance, die die DataCore-Swarm-Technologie in einer einsatzbereiten Hardwareplattform vereint.

Das System wurde konzipiert, um typische Herausforderungen mittelständischer IT-Abteilungen zu adressieren: knappe Personalressourcen, beschränkte Budgets und den Bedarf nach sofort einsetzbaren Lösungen. rapidSWARM SNS lässt sich ohne umfangreiche Projektplanung implementieren, ist unmittelbar produktiv einsetzbar und kann bei Bedarf stufenweise ausgebaut werden.

N-Tec verbindet dabei robuste, energieeffiziente Hardware mit den Sicherheits- und Datenmanagement-Funktionen von DataCore. Daraus entsteht eine Lösung, die gleichermaßen performant wie wirtschaftlich ist. Insbesondere für Einsatzszenarien wie

Was zeichnet Cyber-Resilienz aus?

- Schutz vor Datenverlust, Manipulation und Ransomware
- Schnelle und kontrollierte Wiederherstellung nach Angriffen oder Ausfällen
- Manipulationssichere, revisionsfeste Archivierung (z. B. durch WORM-Technologie)
- Verschlüsselung der Daten im Ruhezustand und während der Übertragung
- Automatische Selbstheilung bei Hardware- oder Speicherausfällen
- Einhaltung regulatorischer und rechtlicher Anforderungen
- Zentrale, intuitive Verwaltung und granulare Zugriffskontrolle

N-Tec rapidSWARM SNS Appliance im Detail

In der heutigen digitalen Landschaft stehen mittelständische Unternehmen vor der Herausforderung, ihre Daten nicht nur effizient zu speichern, sondern auch vor zunehmenden Bedrohungen wie Ransomware zu schützen und gleichzeitig regulatorische Anforderungen wie die *NIS-2*-Richtlinie der EU zu erfüllen. Die **N-Tec** *rapidSWARM SNS Appliance* bietet eine maßgeschneiderte Lösung, die Sicherheit, Skalierbarkeit und Benutzerfreundlichkeit vereint.

Technische Spezifikationen

Die rapidSWARM SNS Appliance basiert auf leistungsstarker Hardware und ist in drei Varianten (Modell S/M/L) mit 25, 50 bzw. 100 TByte erhältlich. Jede Appliance ist mit *Intel XEON Scalable*-Prozessoren, NVMe-Cache und zwei Dual 10/25 Gbit-Ports ausgestattet. Die acht verfügbaren Bays ermöglichen eine flexible Bestückung mit SAS-HDDs, die je nach Kundenbedarf vorkonfiguriert und ausgeliefert werden. Bei steigenden Anforderungen kann das System im Scale-out-Verfahren auf bis zu 2 PByte erweitert werden, indem mehrere Module kombiniert werden.

Software-Integration

Im Kern der rapidSWARM SNS Appliance arbeitet die *Single Node Swarm*-Software von *DataCore*. Diese software-definierte Speicherlösung ermöglicht ein einfaches Management ohne die übliche Komplexität und stellt die Datenintegrität durch einen Secure Agent sicher.

Sicherheitsmerkmale

Die Appliance bietet umfassende Sicherheitsfunktionen:

- **Erasure-Coding:** Internes Erasure Coding schützt vor Datenverlust durch Hardware-Ausfälle.
- **Replikation:** Kombination mehrerer Server ermöglicht durch Replikation vor Ort eine höhere Verfügbarkeit für Backup- und Archivdaten.
- **Asynchrone Replikation:** Eine ausgelagerte Instanz kann über asynchrone Replikation in ein externes Rechenzentrum implementiert werden, um eine geo-redundante Datensicherung gegen Ransomware und lokale Bedrohungen zu gewährleisten.

Preis und Verfügbarkeit

Die N-Tec rapidSWARM SNS Appliance steht in der Regel innerhalb weniger Wochen zur Auslieferung bereit. Die 25-TByte-Lösung (Modell S) ist schlüsselfertig und vorkonfiguriert ab 9.990 Euro netto erhältlich.

Cyber-Resilienz im Mittelstand

Für weiterführende Informationen empfehlen wir die Aufzeichnung unseres Webinars »Cyber-Resilienz im Mittelstand: Hochleistung und Sicherheit für Ihre Daten«. Dieses Webinar wurde in Zusammenarbeit mit Vertretern von DataCore und speicherguide.de durchgeführt. Sie können **die Aufzeichnung hier abrufen.**

Archivierung, Backup-Ziele, Ransomware-Resilienz oder revisionssichere Datenhaltung bietet rapidSWARM SNS eine ausgewogene Balance aus Leistung, Schutz und Bedienkomfort.

Partnerschaft mit Mehrwert: Skalierbar, sicher, zukunftsfähig

Durch die enge Partnerschaft von DataCore und N-Tec entsteht eine integrierte Speicherplattform, die gezielt auf die Bedürfnisse des Mittelstands ausgerichtet ist – vom regionalen Gesundheitsversorger über Finanzdienstleister bis hin zu Industrie- und Forschungseinrichtungen. Das Zusammenspiel von softwaredefiniertem Objektspeicher und deutscher Systemintegrationsexpertise ermöglicht es Unternehmen, ihre Daten sicher, effizient und zukunftsfähig zu verwalten, ohne aufwendige Migrationsprojekte realisieren zu müssen.

Fazit: Resilienz als strategischer Faktor

Cyber-Resilienz ist heute keine freiwillige Maßnahme mehr, sondern eine zwingende Voraussetzung für geschäftskritische IT-Systeme. Mit dem DataCore Single Node Swarm und den schlüsselfertigen, vorkonfigurierten und individuell anpassbaren *rapidSWARM*-Appliances von N-Tec steht mittelständischen Unternehmen eine Lösung zur Verfügung, die maximale Datensicherheit, flexible Skalierbarkeit und unkomplizierte Verwaltung kombiniert. Und dies wenige Wochen nach Bestellung! ■

Weitere Informationen:

N-Tec GmbH
Adalperostrasse 29,
D-85737 Ismaning
Tel. + 49 (0) 89 - 95 84 07-0

Mehr zu N-Tec Single Node Swarm / rapidCore Swarm SNS

www.n-tec.eu/service/hosting-und-cloud/datacore-swarm-sns

Fachhändler für Storage-Systeme

Datagroup Köln GmbH
Schanzenstraße 30, 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 0228/9080 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
Langbaurghstraße 17, 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
Industriestraße 4-6, 61440 Oberursel
Tel. 061 72/936 50, Fax 061 72/93 65 40
www.ins-online.de

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

Topmedia Data Concepts 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
Daimlerring 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

Campus Computersysteme GmbH
Langbaurghstraße 17, D-53842 Troisdorf
Tel. 02241/9411–0
info@campusnet.de,
www.campusnet.de/

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, F
ax 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.bechtle.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-Urloffen
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 EDV-Vertriebs u. Software GmbH
Bunsenstrasse 3, 82152 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@tproneth.de,
www.tproneth.de

Bechtle Network und Security Solutions GmbH
Elisabeth-Schiemann-Bogen 3,
85716 Unterschleißheim
Tel. +49 89 1472764 100
info.bns@bechtle.com,
www.bechtle-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

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-Unternehmungsgruppe GmbH & Co. KG
Kirchplatz 1, 93489 Schorndorf
Tel. 094 67/740 60, Fax 094 67/740 62 90
info@sysob.de,
www.sysob.de

Vom Nischenprodukt zum Standard: All-Flash-Speicher im Überblick

SCHNELLER STORAGE FÜR DAS RECHENZENTRUM

All-Flash-Systeme sind im Primärspeicher zur neuen Normalität geworden. Entscheidend sind die saubere Abgrenzung zu Hybrid-, HDD- und NVMe-only-Architekturen, das Verständnis der technischen Grundlagen sowie ein Überblick über relevante Einsatzfelder und Herstellerlandschaft in Mittelstand und Enterprise.

Karl Fröhlich
speicherguide.de

Ein All-Flash-System ist ein Speichersystem, dessen gesamte produktive Kapazität auf Flash-Medien liegt. Es stellt block-, file- oder objektbasierten Speicher bereit, arbeitet aber ausschließlich mit SSDs oder speziell aufgebauten Flash-Modulen. Klassische Festplatten sind in diesen Systemen nicht mehr Bestandteil der Datenhaltung, höchstens noch als Boot- oder Management-Medium im Hintergrund.

Wichtig ist dabei die Abgrenzung zu einem herkömmlichen Disk-Array, in das einfach statt Festplatten nur SSDs gesteckt wurden. Bereits vor über zehn Jahren wurde dies auf speicherguide.de sehr klar formuliert: Ein All-Flash-System ist kein SATA- oder SAS-Array, in dem zufällig nur SSDs verbaut sind. Solche Systeme bleiben technisch Hybrid-Lösungen, weil ihre Architektur und insbesondere die Plattenkanäle weiterhin für HDD-Profile ausgelegt sind.

Moderne All-Flash-Systeme sind deshalb durchgängig auf Flash optimiert. Typisch sind:

- massiv parallele Controller-Architektur.

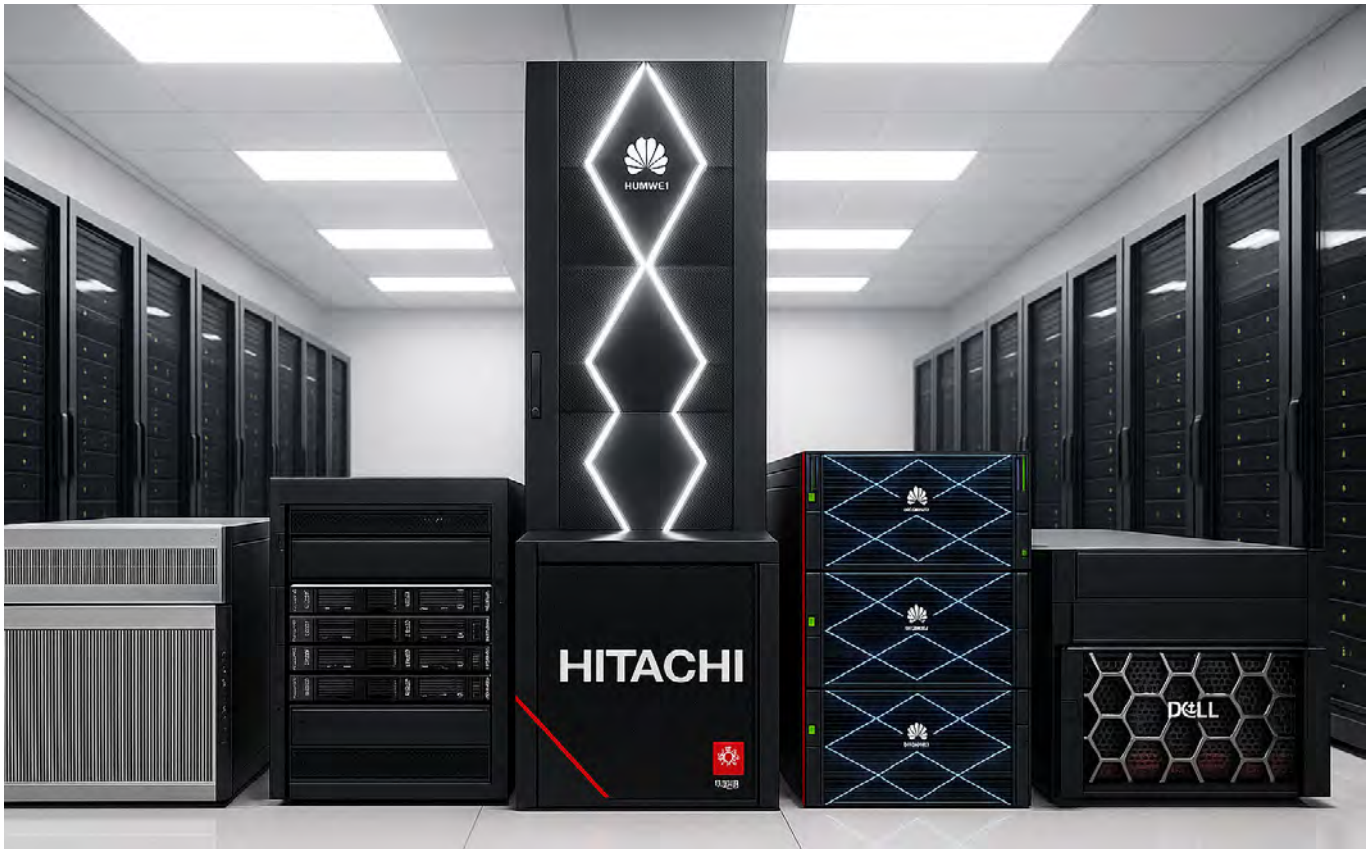


Bild: speicherguide.de und die jeweiligen Hersteller via DALL-E

Bild: Dell

Dell PowerStore als universelles All-Flash-Array mit End-to-End-NVMe für gemischte Block-, File- und vVol-Workloads im Enterprise- und Midrange-RZ.

- Flash-spezifische Funktionen wie Wear-Leveling, Garbage-Collection und Overprovisioning.
- integrierte Datenservices wie Deduplizierung, Kompression, Snapshots und Replikation.
- sehr niedrige Latenzen im Mikrosekunden-Bereich bei hohen IOPS-Raten.

Ob das System über Fibre-Channel, iSCSI, NFS/SMB, NVMe-oF oder als hyperkonvergenter Knoten angebunden ist, ändert nichts an der Grunddefinition: Entscheidend ist das Medium, nicht das Protokoll.

All-Flash: Aktueller Stellenwert im IT-Markt

Marktstudien zeichnen inzwischen ein recht klares Bild:

- Die globale Marktgröße für All-Flash-Arrays wurde für 2024 von **Grand View Research** auf rund 18 bis 19 Milliarden US-Dollar geschätzt, mit Prognosen zwischen gut 66 und über 70 Milliarden US-Dollar bis 2032 bzw. 2033. Die erwarteten jährlichen Wachstumsraten liegen je nach Studie zwischen etwa 16 und knapp 20 Prozent.
- Laut **Verified Market Reports** liegen Schätzungen für den breiteren All-Flash-Markt, in 2024 bei rund 20,6 Milliarden US-Dollar mit deutlichem Wachstum bis 2033.
- Nach Architektur-Segmenten dominieren derzeit klassische Scale-up-Arrays mit knapp der Hälfte des All-Flash-Array-Marktes. Gleichzeitig wachsen laut **Mordor Intelligence** NVMe-oF-basierte, disaggregierte Architekturen mit den höchsten Raten.

In der Praxis bedeutet das: Im Enterprise- und oberen Midrange-Segment ist All-Flash für Primär-Workloads de facto Standard bei Neuanschaffungen. Bei gemischten Workloads oder wenn sehr große Datenmengen kostengünstig untergebracht werden sollen, spielen auch hybride Systeme weiterhin eine Rolle.

All-Flash wandert von klassischen Transaktionsdatenbanken und VDI zunehmend in KI-Pipelines und Analytics. Beispiele sind All-Flash-Objektspeicher wie **Cloudian** *HyperStore Flash* oder **Scality** *Ring XP*, deren Objektspeicher-Architekturen für KI-Workloads in hochskalierenden Umgebungen bis hin zum Exabyte-Bereich ausgelegt sind.

Auch im Sekundär-Storage beginnt All-Flash zu erscheinen, etwa in Backup-Appliances, wenn sehr kurze Sicherungsfenster und kurze Wiederherstellungszeiten gefordert sind, wie aktuelle All-Flash-*DXi*-Systeme von **Quantum** oder die All-Flash-Knoten der *CX8000*-Serie von **Cohesity** zeigen.

Aus wirtschaftlicher Sicht verschiebt sich der Fokus weg von reinen Investitionskosten pro TByte hin zu Gesamtbetriebskosten, Performance pro Kilowatt und Flächeneffizienz. In diesen Kennzahlen liegen All-Flash-Systeme im Primär-Storage deutlich vorn, obwohl HDD auf Kapazitätsebene günstiger bleibt.

All-Flash-Systeme im Überblick

An den Top-Playern für klassische All-Flash-Arrays kommt man aktuell kaum vorbei. Aus heutiger Sicht sind die folgenden drei US-Hersteller besonders wichtig:

Dell Powerstore/Powermax: All-Flash für alle Segmente

Dell liegt beim Umsatz mit All-Flash-Systemen laut IDC seit Jahren vorne und bezeichnet sich selbst auf Basis dieser Zahlen als Nummer 1 bei All-Flash-Storage.

Für den Alltagsbetrieb in Enterprise- und größeren Midrange-Umgebungen ist vor allem *Dell PowerStore* das zentrale All-Flash-Array:

- End-to-End-NVMe-Architektur, aktive Dual-Controller, sehr niedrige Latenzen für Block-, File- und vVol-Workloads.
- Positioniert als universelle Plattform zwischen Einstiegs-Storage und Highend-Systemen wie *PowerMax* und damit in vielen Rechenzentren eine verbreitete Standardplattform für Primär-Storage.

Powerstore bietet außerdem Always-on-Datenreduktion, Scale-out-Ausbau und mit *AppsON* die Möglichkeit, Workloads direkt auf dem Array auszuführen. Mit Powermax adressiert der Hersteller das Highend-Segment mit hohen IOPS-Werten, Mainframe-Anbindung und erweiterten Data-Protection-Funktionen für Tier-0-Anwendungen. In der Summe dominiert Dell den externen Enterprise-Storage-Markt insgesamt

Bild: Hitachi Vantara

Hitachi VSP als NVMe-basiertes All-Flash-Array für unternehmenskritische Block-Workloads vom Midrange- bis in den Highend-Bereich.

und hat mit Powerstore eine sehr breite installierte Basis im All-Flash-Segment.

Netapp – AFF A-Series & ASA: All-Flash für Unified & SAN

NetApp ist traditionell stark im Primär-Storage und wird im Gartner-»*Magic-Quadrant für Primary Storage Platforms*« seit vielen Jahren durchgehend als »Leader« geführt.

Im All-Flash-Umfeld sind zwei Produktlinien entscheidend:

- AFF A-Series: Unified-All-Flash-Arrays für Block, File und teilweise Objekt, mit ONTAP als Data-Management-Schicht und Unterstützung für NVMe/FC und NVMe/TCP.
- ASA (All-Flash SAN Arrays): Block-only-Varianten auf AFF-Basis, optimiert für klassische SAN-Workloads wie Datenbanken und VMware, mit sehr hoher Verfügbarkeit und Kapazitätseffizienz.

Netapp spielt beim weltweiten externen Storage-Umsatz zwar »nur« im oberen Mittelfeld hinter Dell und HPE, ist aber speziell bei All-Flash-Arrays für Unified- und SAN-Umgebungen einer der am weitesten verbreiteten Anbieter im Enterprise-Segment.

Pure Storage – FlashArray//X & //C: Pure Storage gehört zu den wenigen großen Herstellern, die ihr Kerngeschäft fast vollständig auf All-Flash-Arrays ausgerichtet haben. Die *FlashArray*-Familie ist das zentrale Produkt:

- FlashArray//X: NVMe-basiertes High-Performance-All-Flash-Array für Tier-0/Tier-1-Workloads mit einheitlichem Block- und File-Storage und sehr niedrigen Latenzen.
- FlashArray//C: kapazitätsoptimiertes All-Flash-Array auf NVMe-Basis, oft mit QLC-Flash, für kostensensitivere, aber performancekritische Tier-2-Workloads.

Pure setzt auf eine eigene *DirectFlash*-Architektur, bei der kundenspezifische NVMe-Module direkt von der *Purity*-Software angesteuert werden. Laut Hersteller sorgt dies für besonders niedrige Latenzen, hohe IOPS und eine hohe Energie- und Flächeneffizienz im Vergleich zu klassischen SSD-Arrays. Dies bringt allerdings eine stärkere Herstellerbindung mit sich, da sich Module und Funktionalität nicht durch Standard-SSDs anderer Anbieter ersetzen lassen.

All-Flash-Arrays aus Japan und China

Als Ergänzung zu den US-Anbietern lassen sich vier Nicht-US-Hersteller mit klaren All-Flash-Array-Portfolios benennen:

Hitachi Vantara VSP: All-Flash von Midrange bis Highend

Wichtige All-Flash-Produkte:

- *Virtual Storage Platform 5000 Series (VSP 5200/5600)*: Highend-All-Flash-Plattform mit durchgängiger NVMe-Architektur, ausgelegt für sehr hohe IOPS und niedrige Latenzen. Hitachi positioniert die VSP-5000-Serie explizit als NVMe-Flash-Array für Enterprise-Workloads.
- *Virtual Storage Platform F Series*: Midrange-All-Flash-Arrays (Modelle wie VSP F1500, F900, F800, F700), fokussiert auf hohe Verfügbarkeit und All-Flash-Performance für geschäftskritische Anwendungen.
- *Virtual Storage Platform E Series*: Midrange-Systemfamilie mit Hybrid- und All-Flash-Varianten. Modelle wie VSP E590, E790 und E990 werden als All-NVMe-Midrange-Flash-Arrays vermarktet und adressieren klassische Block-Workloads im mittleren Segment.
- *VSP One Block*: Relativ neue, skalierbare NVMe-All-Flash-Plattform für Block-Storage im Midrange-Bereich, mit Active-Active-Controllern und Ausbau bis zu vielen Appliances pro Verbund.

Damit deckt Hitachi den All-Flash-Bereich von Midrange bis Highend durchgängig ab und bietet eine einheitliche Architektur mit Funktionen wie integrierter Storage-Virtualisierung, Data-Reduction-Services und Optionen für Mainframe- und Open-Systems-Umgebungen.

Huawei OceanStor Dorado: All-Flash für Block, File, Objekt

Huawei bündelt seine All-Flash-Produktlinie unter dem Namen *OceanStor Dorado All-Flash Storage*:

- *OceanStor Dorado 3000 V6*: Einstiegs-All-Flash-System für kleine und mittlere Unternehmen, mit SSD-only-Architektur und End-to-End-NVMe-Design für schnellen Datenzugriff.
- *OceanStor Dorado 5000/6000*: Konvergente Midrange-All-Flash-Systeme für Block-, Datei- und S3-fähige Objekt-Workloads, ausgelegt auf hohe IOPS, niedrige Latenzen und breiten Enterprise-Einsatz.
- *OceanStor Dorado 8000/18000*:

Highend-All-Flash-Arrays mit sehr hohen IOPS-Werten und extrem niedriger Latenz, konzipiert für geschäftskritische Primärdaten sowie große KI- und Analytics-Workloads.

Huawei adressiert damit das komplette Spektrum vom KMU-System bis zur großen, konvergenten Enterprise-Plattform. In der Diskussion steht der Hersteller immer wieder aufgrund seiner Herkunft und der geopolitischen Lage. Wie wir hören, stehen demgegenüber aber, oft eine umfangreiche Unterstützung sowie Service-Leistungen und meist attraktive Einkaufskonditionen.

Fujitsu ETERNUS AF: All-Flash-Arrays mit automatisierter QoS

Fujitsu bietet mit der ETERNUS AF-Serie klassische All-Flash-Arrays an:

- *ETERNUS AF150 S3*: Einstiegs-All-Flash-Array, gedacht als kostengünstiger Einstieg in Flash für Tier-1-Applikationen.
- *ETERNUS AF250 / AF250 S2*: All-Flash-Systeme für kleine und mittlere Umgebungen, mit Kapazitäten im Hundert-TByte-Bereich und Response-Zeiten unter 1 ms, typischerweise für virtuelle Server, Datenbanken und VDI.
- *ETERNUS AF650*: All-Flash-System für größere Datenbanken und anspruchsvollere Enterprise-Workloads, mit hohen IOPS-Werten und FC/iSCSI-Anbindung.

Die Eternus-AF-Familie fokussiert damit vor allem auf klassische SAN-Szenarien in KMU und gehobenem Mittelstand. Ergänzend bieten die Systeme automatisierte Quality-of-Service-Funktionen, Thin-Provisioning sowie – je nach Modell – Deduplizierung und Kompression zur besseren Ausnutzung der Flash-Kapazität. Optional verfügbare Storage-Cluster mit transparentem Failover und Remote-Copy-Optionen adressieren hochverfügbare Zwei-Standort-Umgebungen.

Lenovo Thinksystem DM/DE: All-Flash für SAN & Unified

Lenovo deckt den All-Flash-Array-Markt mit zwei Hauptlinien ab, die unterschiedliche Einsatzszenarien adressieren:

- *ThinkSystem DM Series All-Flash*: Die DM-Serie (u. a. DM5000F, DM5100F, DM7000F, DM7100F) sind skalierbare, Unified-All-Flash-Systeme für File-, Block- und teilweise Objekt-Workloads. Basis ist *NetApps ONTAP*, sodass Funktionen wie Deduplizierung, Kompression, Snapshots, Replikation, FabricPool-Tiering und Ransomware-Schutz integriert sind. Die Systeme werden als All-Flash-Variante mit NVMe-SSDs angeboten und zielen auf Enterprise-Workloads wie Datenbanken, VDI, AI/Analytics und virtuelle Serverfarmen.
- *ThinkSystem DE Series All-Flash*: Die DE-Serie (DE4000F, DE6000F, DE6400F/DE6600F) bildet die All-Flash-SAN-Familie. Sie ist für blockbasierte Workloads in mittelgroßen bis großen Umgebungen ausgelegt, mit IOPS-Werten bis in den Millionenbereich, Latenzen unter 100 Mikrosekunden und Durchsatzraten bis zu mehreren Dutzend GByte/s. Die Systeme unterstützen verschiedene Protokolle wie FC, iSCSI sowie NVMe-over-Fabrics und eignen sich für Mixed-Workloads, Big-Data-Analytics, HPC und KI-Anwendungen.

Lenovo ist damit als Nicht-US-Hersteller im All-Flash-Segment sowohl im Unified- als auch im klassischen SAN-Bereich breit aufgestellt und global präsent – vor allem im Enterprise- und gehobenen Mittelstandsmarkt. Diskussionen um die chinesische Herkunft fallen leiser aus, da Lenovo vor allem Standard-IT statt kritischer Netzinfrastruktur liefert.

Huawei OceanStor Dorado als All-Flash-Storage-Plattform mit End-to-End-NVMe für Block-, File- und S3-Objekt-Workloads in Enterprise-Umgebungen.

Deutsche Anbieter von All-Flash-Systemen

N-Tec: All-Flash für KMUs

N-TEC positioniert sich als deutscher Lösungsanbieter, der individuelle All-Flash-Systeme auf Basis bewährter Hardware-Plattformen aufbaut. Als Plattformen dienen unter anderem All-Flash-Arrays wie die *XCubeFAS*-Serie des Herstellers **QSAN**, die N-Tec als energieeffiziente und leistungsstarke All-Flash-Lösungen für transaktions-

RNT BigFoot Flash als hochdichtes All-Flash-System mit bis zu mehreren Dutzend SSDs in 2U für leistungsintensive Virtualisierungs- und Datenbank-Szenarien.

intensive Workloads im Mittelstand vermarktet.

Ein zweites Standbein sind die eigenen *rapidNAS JSS*-Systeme, die in Kombination mit der SDS-Software **Open-E** *JovianDSS* zu hochverfügbaren All-Flash-Konfigurationen ausgebaut werden können – bis hin zu aktiven Metro-Clustern mit niedrigen Latenzen und synchroner Spiegelung.

RNT Rausch Bigfoot/Sasquatch: schnell und flexibel

RNT Rausch adressiert All-Flash-Anforderungen sowohl mit eigenen Hardware-Plattformen als auch mit integrierten SDS-Lösungen. Die *BigFoot Flash*-Familie (Modelle *BigFoot Flash 1/20, 1/20N* und *2/52*) ist als All-Flash-Storage mit bis zu über einer Million IOPS, bis zu 52 SSDs in 2U und optionalen NVMe-Konfigurationen ausgelegt und zielt auf Performance-Szenarien wie VDI, Analytics oder Medien-Workloads.

Zusätzlich bietet RNT unter der Marke *Sasquatch* integrierte All-Flash-SDS-Lösungen »powered by Huawei«, etwa *Integrated All-Flash-Storage S* und *M*. Diese Systeme kombinieren Huawei-Dorado-All-Flash-Arrays mit einer vorkonfigurierten SDS-Schicht und richten sich an mittelständische und Enterprise-Umgebungen mit virtualisierten Workloads und Enterprise-Applikationen.

Eurostor ES-6600 / ES-8724JASA: All-Flash mit hoher Dichte

EUROstor tritt als deutscher Hersteller maßgeschneiderter Storage-Server und RAID-Systeme auf und bietet mehrere Plattformen, die sich explizit als All-Flash-Arrays konfigurieren lassen. Die Serie *ES-6600 All Flash RAID* erlaubt Konfigurationen mit 24 2,5-Zoll-SSDs im Grundchassis, erweiterbar auf bis zu 250 SSDs, mit 12-Gbit/s-SAS im Backend und 16/32-Gbit/s-Fibre-Channel oder SAS zum Host – ausgelegt als kosteneffiziente All-Flash-SAN-Lösung.

Zusätzlich unterstützen die ES-6600-Arrays Single- oder Dual-Controller, flexible RAID-Level in einem Verbund und ein webbasiertes Management für die Konfiguration und Überwachung. Im oberen Leistungsbereich positioniert Eurostor unter anderem das Full-NVMe-System *ES-8724JASA-2U*, ein All-Flash-Metro-Cluster auf Basis von Open-E JovianDSS mit bis zu rund 737 TByte NVMe-Kapazität in 2U, das sich an Rechenzentren, Managed-Service-Provider und anspruchsvolle Virtualisierungs- und Datenbank-Workloads richtet und durch ZFS-Prüfsummen sowie Snapshots ein hohes Maß an Datenintegrität und Verfügbarkeit bietet.

Thomas-Krenn OSS Performance Plus: All-Flash & Metro-Cluster

Thomas-Krenn ist als deutscher Server- und Storage-Hersteller mit mehreren All-Flash-Systemlinien präsent. Unter den *Open Storage Systems* (OSS) findet sich etwa das 2U-All-Flash-System OSS Performance Plus, das bis zu 24 2,5-Zoll-SSDs und rund 368 TByte Kapazität für maximale Performance in kompakter Bauform bereitstellt.

Parallel dazu bietet Thomas-Krenn schlüsselfertige All-Flash-Appliances auf Basis von Open-E JovianDSS an. Die Lösung *Open-E RA1112 (All-Flash) Metro Cluster* kombiniert zwei kompakte All-Flash-Knoten zu einem synchron gespiegelten Metro-Cluster für hochverfügbare Datenhaltung und nutzt ZFS samt umfangreicher Snap- und Integritätsfunktionen.

Für größere Szenarien steht mit *RA1224-AF* ein All-Flash-Cluster mit höherer Laufwerksdichte und bis zu 100-Gbit/s-Ethernet zur Verfügung, der explizit für Data-Center-Workloads konzipiert ist.

Fast LTA: Modularer All-Flash mit hoher Sicherheit

FAST LTA mit Sitz in München positioniert sich als Spezialist für sichere Speicherlösungen für Backup und Archivierung. Herzstück ist das *Silent Brick*-System mit modularen Medien wie *Silent Brick Plus* und *Silent Brick Pro*. Silent Brick Plus ist als All-Flash-Medium mit zwölf SSDs ausgelegt, eignet sich laut Hersteller als erste Backup-Instanz und bietet hohe Performance für Primär-Backups, etwa als *Veeam*-Target.

Der neue Silent Brick Pro setzt zusätzlich auf NVMe-Flash und erreicht in Verbindung mit dem *Controller X* Datenraten von mehreren GByte/s, womit auch sehr kurze Backup-Fenster und schnelle Restores adressiert werden. Das Silent-Brick-System deckt damit als deutsche Lösung den Bereich All-Flash vor allem auf der Sekundär-Storage-Ebene ab und kombiniert hohe Sicherheit mit Funktionen wie Air-Gap, Immutability und mehrstufiger Paritätsabsicherung. ■

Weiterführende Infos:

Primärspeicher – zwischen All-Flash und hybrid

DATACORE™

Solving **Data Challenges** *at* **Every Level**

More Solutions. *More Possibilities,* **One DataCore.**

Your Data, Our Priority

Daten vorbereiten, I/O-Pfade verkürzen, GPU-Zeit ausnutzen

KI IM RECHENZENTRUM: STORAGE NEU DENKEN, ENGPÄSSE VERMEIDEN

Viele Unternehmen starten KI-Projekte, doch es entstehen bislang nur wenige belastbare Ergebnisse. Oft scheitert es an Compliance, Datensilos und überhöhten Erwartungen. Gefordert ist eine On-Prem-Architektur, die Daten unternehmensweit verfügbar macht und die Pipeline optimiert: kuratieren, indizieren, vektorisieren. Kurze Wege über NVMe, RDMA, GPUDirect sowie CXL-Pooling und skalierende Dateisysteme erhöhen Durchsatz und senken GPU-Wartezeiten.

Karl Fröhlich
speicherguide.de

Unternehmensinterne KI-Vorhaben scheitern überraschend oft. Drei Muster tauchen immer wieder auf: »Erstens bremsen Compliance- und Sicherheitsbedenken, wenn Herkunft, Klassifizierung und Zugriffsrechte der Daten unklar sind«, erklärt **Wolfgang Stief** von **Stief Consulting**. »Zweitens blockieren Datensilos aus vergangenen IT-Generationen die Versorgung der Modelle mit relevanten, aktuellen Informationen. Drittens fehlt es häufig an begrifflichem Fundament und realistischen Erwartungen.« KI ersetzt keine Teams auf Knopfdruck. Sie braucht Kulturarbeit, konkrete Use-Cases und eine Datenbasis, die technisch und organisatorisch sauber erschlossen ist.

Datenvorbereitung ist Pflichtprogramm

Für KI genügt es nicht, Daten nur »zu haben«. Sie müssen über den gesamten Lebenszyklus kuratiert werden: auffinden, bereinigen, klassifizieren, indizieren, anreichern, versionieren, rechtlich einordnen und – ganz zentral – vektorisieren. Modelle arbeiten letztlich mit Einbettungen als Vektordaten. »Ohne diese Vorarbeit bleiben Ergebnisse unzuverlässig und anfällig für Halluzinationen«, sagt Stief. »Moderne Plattformen unterstützen Teilaufgaben wie automatisches Tagging oder Vorschläge zur Klassifizierung, dennoch bleibt menschliche Validierung notwendig.« Ziel sei eine demokratisierte Datensicht über Silogrenzen hinweg, die den Zugriff für Training und Inferenz organisatorisch erlaubt und technisch beschleunigt.

LLM-Begriffe knapp eingeordnet

Große Sprachmodelle entwickeln sich zu multimodalen Systemen, die Text, Bild, Audio und weitere Signale verarbeiten. Für viele Unternehmensprozesse ist Multimodalität sinnvoller als reine Textmodelle. *Retrieval-Augmented Generation* (RAG) ergänzt Modellwissen um aktuelle, interne Quellen. Parameterzahl, Kontextfenster und Token-Durchsatz sind Qualitätsfaktoren, jedoch nur im Zusammenspiel mit sauber vorbereiteten, zugänglichen Daten und einer passenden Architektur wirklich wirksam.

Der KI-Lebenszyklus bestimmt das I/O-Profil

Entlang der Pipeline ändern sich Lastcharakteristiken deutlich:

- Sammeln und Aufbereiten: vorwiegend sequentielle, schreibbetonte Workloads auf NVMe-SSDs. Deduplizieren, Indizieren und Vektorisieren erfordern zusätzlich CPU- und Netzressourcen.
- Training: leseintensiv mit vielen Random-Reads. Kritisch sind kurze

Bild: speicherguide.de via DALL-E

Für KI müssen Storage-Systeme nicht nur schnell, sondern auch compliant und sicher sein.

Wege zwischen NVMe und GPU-Speicher wie HBM. Checkpointing ist ein Kostentreiber, weil GPUs während des Schreibens nur begrenzt arbeiten und beim Laden warten. Je schneller Checkpoints weggeschrieben und wieder eingelesen werden, desto besser die Auslastung.

- Inference und RAG: dominiert von latency-sensitiven Random-Reads. Hier wird Storage zum häufigsten Engpass. Caching-Strategien und ausreichender Arbeitsspeicher für Zwischenergebnisse sind entscheidend, damit Antworten interaktiv bleiben.

Eine Architektur, die diese Phasen sauber trennt und passend auslegt, ist stets im Vorteil gegenüber generischen »One-Size-Fits-All«-Ansätzen.

Speicher- und Interconnect-Hierarchie: die Memory-Wall ist real

Vom Register über CPU-Caches und DDR bis zu HBM, NVMe-SSDs und letztlich Band sind die Bandbreiten- und Latenzsprünge enorm. Für KI zählt deshalb nicht nur Kapazität, sondern vor allem die Nähe der Daten zum Rechenkern. Relevante Bausteine:

- HBM und GPU-Interconnects wie NVLink für sehr hohe Bandbreiten im Knoten.
- PCIe Gen5/Gen6 als Systembus, perspektivisch Gen7. NVMe 2.x bringt Funktionen wie *Zoned Namespaces* (ZNS) und verbessert Queuing.
- NVMe-oF über RDMA oder TCP, plus (R)DMA und GPUDirect, um Umwege über die CPU zu vermeiden und Datenpfade zu verkürzen.
- CXL als Enabler für disaggregierten, composable Memory und Gerätepools über Chassis-Grenzen hinweg. Das eröffnet Spielräume bei Inferenz, etwa für größere Kontextfenster durch Memory-Pooling.

Die praktische Regel: Daten so nah wie möglich an die GPU bringen, Engpässe früh identifizieren und bei Checkpoints lokale NVMe im GPU-Server berücksichtigen, wenn die Software-Stacks dies unterstützen. Das reduziert Wartezeiten und steigert die GPU-Auslastung spürbar.

> »KI ist nicht gleich KI. 95 Prozent der KI-Projekte scheitern, meist, weil ohne Plan und der richtigen Strategie agiert wird.«
>
> **Wolfgang Stief, Stief Consulting**

Bild: Wolfgang Stief

Verteilte Dateisysteme und Standard-Protokolle

Skalierung entsteht durch Parallelisierung. Verteilte Dateisysteme trennen Metadaten von Nutzdaten und erlauben viele parallele Datenströme zu den Speicherzielen. In der Praxis kommen je nach Umgebung unter anderem *Ceph*, *BeeGFS*, *Lustre* oder *Weka* zum Einsatz. Auch *pNFS/NFSv4.2* kann mit passenden Erweiterungen parallel arbeiten und ist operativ oft einfacher handhabbar. Wichtig ist weniger der Markenname als die Fähigkeit, Metadaten-Hotspots zu vermeiden, parallele Clients effizient zu bedienen und die vorhandenen Netze auszureizen.

Netzwerke: Latenz und Durchsatz als Stellhebel

KI- und HPC-Workloads profitieren von verlustarmen, schnellen Fabrics. *InfiniBand* gilt weiter als Referenz für niedrige Latenzen, Ethernet mit 200G/400G/800G ist breit verfügbar und dank RDMA-Varianten leistungsfähig. Initiativen wie *UltraEthernet* zielen auf deterministischere Performance im Ethernet-Ökosystem. Entscheidend ist ein Ende-zu-Ende-Design: Adapter, Switches, Treiber und Protokolle müssen zusammenpassen, sonst verpufft theoretische Bandbreite in Pufferung und Retransmits.

Beschaffung: Benchmarks richtig lesen

Kennzahlen helfen, wenn man sie korrekt einordnet. *MLPerf* bietet KI-nahe Benchmarks, *SPC-2* misst sequenzielle Throughput-Szenarien und der *IO500* vergleicht parallele Filesystem-Leistung. Ergebnisse sind nur innerhalb derselben Benchmark-Version sinnvoll vergleichbar. Zudem gilt: Kontext ist alles. Ein Test, der auf maximale Sequenzen ausgelegt ist, sagt wenig über RAG-Workloads mit vielen kleinen Random-Reads. Praxisnahe PoCs (Proof of Concept) mit eigenen Daten und realistischen Zugriffsmustern bleiben die beste Entscheidungsgrundlage.

Governance, Backup und Archiv

Trainingsdaten und Modelle lassen sich in vielen Fällen reproduzieren, weshalb ein klassisches Langzeit-Archiv laut IT-Experte Stief nicht immer zwingend ist: »Unverzichtbar sind jedoch Dokumentation, Nachvollziehbarkeit und Daten-Governance. Besonders RAG-Quellen, Konfigurationen, Prompts, Embedding-Versionen und Checkpoints sollten gesichert und versioniert werden. Regulatorische Anforderungen wie der EU-AI-Act adressieren Herkunft, Qualität und Eignung der Daten. Wer hier sauber arbeitet, reduziert Compliance-Risiken und vereinfacht spätere Audits.«

Praktische Leitplanken für Architekturentscheidungen

- **Use-Case konkretisieren:** Inferenz, RAG, Fine-Tuning und volles Training stellen sehr unterschiedliche Anforderungen. Die teuerste Komponente ist fast immer die GPU-Zeit. Alles, was Wartezeiten verringert, spart Geld.
- **Datensicht vereinheitlichen:** Silo-übergreifende Indizes, ein konsistentes Rechte- und Rollenkonzept und klare Data-Lineage sind notwendige Voraussetzungen.
- **Datenwege verkürzen:** Lokale NVMe für Checkpoints, RDMA-fähige

Pfade, GPUDirect-fähige Stacks. Zusätzlich ausreichend DRAM für Zwischenstände bei der Inferenz einplanen.

- **Skalierung planen:** Netzwerk-Uplinks, Queue-Tiefen, Metadaten-Services und Anzahl paralleler Clients gemeinsam betrachten.
- **PoC statt Prospekt:** Herstellerangaben sind Anhaltspunkte. Die Validierung mit eigenen Daten und Workloads ist am Ende ausschlaggebend.

Storage für KI

Daten nur sammeln reicht nicht. Daten müssen (unter anderem):

- kuratiert,
- klassifiziert,
- sortiert,
- indiziert und angereichert,
- vektorisiert sowie
- demokratisiert werden.

Und das nicht nur schnell, sondern auch noch compliant und sicher – außer es macht nichts aus, wenn zum Beispiel Röntgenbilder und Kreditanträge im Darknet ausgewertet werden.

Quelle: Stief Consulting

Fazit: KI-Erfolg ist Datenarbeit: Pipeline, I/O-Pfade und Storage im Griff

KI im Rechenzentrum ist kein rein »rechnerisches« Thema, sondern ein datengetriebenes. »Wer die Pipeline von der Rohdatenaufnahme über Vektorisierung und Indizierung bis zu Training und Inferenz technisch wie auch organisatorisch beherrscht, holt Performance aus den GPUs heraus und erhält reproduzierbare, belastbare Ergebnisse«, meint Stief. »Der Schlüssel liegt in konsequentem Datenmanagement, intelligenten I/O-Pfaden und einer Storage-Architektur, die den realen Zugriffsmustern folgt.« So wird KI praktikabel, auditierbar und wirtschaftlich – und On-Prem-tauglich, ohne auf Cloud-Spezifika vertrauen zu müssen. ■

Veeam Immutable Backup:
Jetzt auch auf EUROstor Server mit Open-E

ES-8700 12 Slot Server mit Open-E JovianVHR Software

Beispielkonfiguration:
2 HE Rack Server mit 16-CORE AMD CPU,
192 GB RAM, 2 x 25 GbE Ports,
voll bestückt mit 10 x 14 TB NL-SAS Disks,
damit ca. 91,7 TiB verfügbare Kapazität
bei einem RAID-Z2 (entspricht RAID6),
Open-E JovianVHR vorinstalliert
auf M.2 SSDs,
3 Jahre Open-E Standard Support

€ 10.290,-
exkl. MwSt.

€ 12.245,10
inkl. MwSt.

Für alle Veeam-Nutzer, die das immutable Backup auf einem „Linux Hardened Repository" als **Schutz vor Ransomware** nutzen wollen.

Open-E JovianVHR ist eine Veeam qualifizierte Softwareversion von Open-E, die die **Vorteile des ZFS Filesystems** mit der **Unveränderlichkeit der Daten** durch das Veeam Linux Hardended Repository verbindet.

Die Lizenz ist kostenlos, und der obligatorische Support durch Open-E ist zu moderaten Preisen erhältlich.

Ebenso erhältlich bei EUROstor:

- **ES-8700J Storageserver** mit **Open-E JovianDSS** für NAS (NFS und CIFS/SMB), iSCSI und optional FC.
- auch als **Active/Active Cluster** lokal oder als **Metro-Cluster** über zwei Standorte
- **OODP Server** (On & Off-Site Data Protection) als **snapshotbasierte Sicherung** an einen anderen Standort

Gerne erstellen wir ein maßgeschneidertes Angebot für Sie.

Für alle Systeme gilt:

- **ZFS 2.0 Filesystem**: maximale Datenintegrität und Schutz vor „Stealth Errors" durch Check-Summen-Prüfung und Disk-Scrubbing.
- umfangreiche Snapshot- und Replikationsfunktionen ohne Zeitverlust und vorreservierte Kapazität
- Kompression, Deduplizierung & Thin Provisioning
- eine **intuitive Web-GUI** erlaubt einfaches Management ohne Spezialkenntnisse.

Alle Storage-Systeme aus einer Hand:

EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unser Portfolio umfasst RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, allgemein einsetzbaren Servern, z.B. für die Server-Virtualisierung.

Registrieren Sie sich einfach unter www.EUROstor.com/Newsletter,

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt – E-Mail: Info@EUROstor.com – Tel.: +49 (0)711 70 70 91 70

Studien-Update 2025: Kapazitäten, Standorte, Energie, Politik

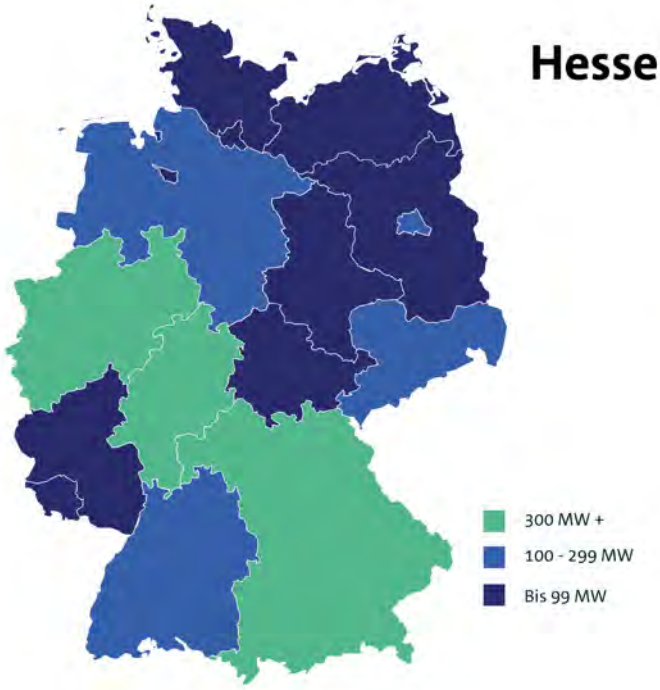
BITKOM-STUDIE: KI MACHT DRUCK AUF DEUTSCHLANDS RECHENZENTREN

KI und Cloud treiben den Ausbau der Rechenzentren in Deutschland. Laut Bitkom und Borderstep Institut wächst die IT-Anschlussleistung 2025 auf 2,98 GW, überschreitet Anfang 2026 die 3-GW-Marke und peilt bis 2030 5 GW an. KI-Kapazitäten vervierfachen sich auf 2,02 GW (40 %). Frankfurt bleibt der Hub. Engpässe: Energiepreise, Netze, Genehmigungen.

Karl Fröhlich
speicherguide.de

Bild: speicherguide.de via DALL-E

Der Befund ist deutlich: KI-Workloads und Cloud-Angebote sind der neue Taktgeber des Rechenzentrums-Ausbaus. Nach Angaben von **Bitkom** und **Borderstep Institut** stehen KI-Rechenzentren aktuell für rund 15 Prozent der in Deutschland installierten Leistung, bis 2030 sollen es 40 Prozent sein. Die dafür genannte IT-Anschlussleistung steigt von derzeit 530 MW auf prognostizierte 2.020 MW. Parallel klettert die gesamte Datacenter-Leistung 2025 auf 2,98 GW, die 3-GW-Marke fällt Anfang 2026. Bis 2030 stehen 5 GW im Raum, womit sich die Kapazitäten gegenüber 2024 nahezu verdoppeln würden. Für Planer, Betreiber und Beschaffer in mittleren bis großen Umgebungen zeichnet sich damit ein Investitions- und Konsolidierungszyklus ab, der Standortwahl, Energie-Beschaffung, Kühlstrategie und Netz-Anbindung neu gewichtet. Zu diesem Ergebnis kommt



Hessen bleibt RZ-Standort Nr. 1

Rang	Bundesland	Aktuell	Angekündigt*
1	Hessen	1.131	1.805
2	Bayern	420	95
3	Nordrhein-Westfalen	378	750
4	Baden-Württemberg	233	64
5	Berlin	146	220
6	Niedersachsen	134	64
7	Sachsen	132	32
8	Hamburg	91	20
9	Rheinland-Pfalz	79	534
10	Sachsen-Anhalt	62	105
11	Brandenburg	44	888
12	Schleswig-Holstein	44	19
13	Thüringen	26	0
14	Meck.-Vorpommern	20	1.000
15	Bremen	19	0
16	Saarland	17	0

Grafik: Bitkom

Innerhalb von Deutschland ist nach wie vor die Region Frankfurt/Rhein-Main der Hotspot für RZ. Die Region wird ihre führende Position in den nächsten Jahren weiter ausbauen.

die Studie »*Rechenzentren in Deutschland: Aktuelle Marktentwicklungen – Update 2025*«.

Server werden effizienter, aber Energiebedarf steigt

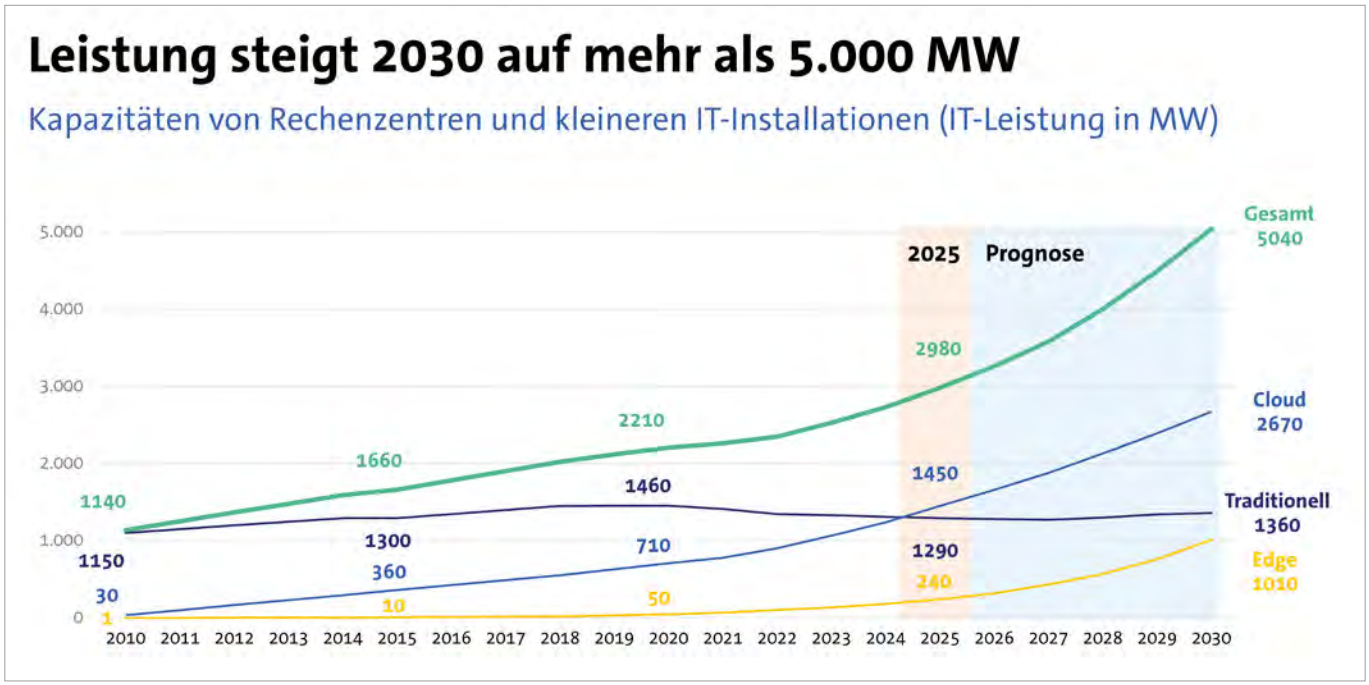
Der Strombedarf der Rechenzentren liegt 2025 bei 21,3 TWh, nach 20 TWh im Jahr 2024 und 12 TWh im Jahr 2015. Rund zwei Drittel entfallen auf die IT-Infrastruktur – Server, Speicher und Netzwerktechnik – ein Drittel auf die Gebäudeinfrastruktur mit Kühlung und unterbrechungsfreier Stromversorgung. Die verwendeten IT-Systeme werden effizienter: Standard-Server verbesserten sich zwischen 2017 und 2022 im Mittel um 26 Prozent pro Jahr. »Die Energieeffizienz von Rechenzentren hat in den vergangenen Jahren deutlich zugenommen, und sie wird angesichts steigender Stromkosten und wachsender Anforderungen durch KI weiter an Bedeutung gewinnen«, sagt Bitkom-Hauptgeschäftsführer **Dr. Bernhard Rohleder**. Effizienz senkt Kosten und Emissionen, ändert aber nichts daran, dass KI-Stacks die absolute Last nach oben schieben.

Deutscher RZ-Schwerpunkt im Raum Frankfurt

Gezählt werden derzeit rund 2.000 Standorte über 100 kW, darunter etwa 100 Anlagen mit mehr als 5 MW. Die größten hundert Rechenzentren liefern bereits die Hälfte der nationalen Leistung. Unangefochtener Schwerpunkt ist der Raum Frankfurt mit gut 1,1 GW, flankiert von Bayern und Nordrhein-Westfalen. Dass Frankfurt mit rund 14 Prozent pro Jahr am schnellsten wächst, liegt an der Anbindung an **DE-CIX**, der dichten Carrier- und Colocation-Landschaft sowie einem reifen Partner-Ökosystem. Das Rhein-Main-Cluster dehnt sich nach Rheinland-Pfalz und Bayern aus, während Berlin-Brandenburg als zweiter Hub sichtbar zulegt. In der Pipeline stehen Projekte mit mehr als 1.800 MW im Raum Frankfurt, 888 MW in Brandenburg und 480 MW in Nierstein. Diskutiert wird zudem ein Vorhaben um die Größenordnung von 1.000 MW in Dummerstorf. Ob diese Projekte Realität werden, entscheidet sich an Planungsrecht, Netzausbau, Flächenverfügbarkeit und lokaler Akzeptanz.

Effizienter, aber hungriger: KI treibt den Strombedarf nach oben

Treiber Nummer eins bleibt »Cloud-Computing« für KI und klassische Dienste. Cloud-Infrastrukturen steigen 2025 um rund 17 Prozent auf 1.450 MW und machen damit knapp die Hälfte der Kapazitäten aus. Edge-Rechenzentren gewinnen an Dynamik, liegen mit etwa 240 MW aber noch auf kleiner Basis. Klassische Enterprise-Rechenzentren bleiben relevant, zeigen jedoch einen rückläufigen Trend. Die Botschaft: Latenz-sensible Workloads rücken näher an den Nutzer, alles andere wandert in hochverdichtete, skalierbare Umgebungen. Technisch wird effizienter gearbeitet, die absolute Last steigt dennoch. Der Großteil entfällt weiterhin auf Server, Storage und Netz, die Gebäudeinfrastruktur folgt wegen Kühlung und USV. Effizienzgewinne dämpfen den Anstieg, kompensieren aber die KI-bedingten Leistungsdichten nicht. Konsequenz: Kühlkonzepte, Strompfade und Abwärme-Nutzung rücken ins Zentrum der Planung, PUE und Betriebskosten bleiben die Taktgeber.



Grafik: Bitkom

Anfang 2026 soll erstmals die Marke von 3.000 Megawatt und 2030 von 5.000 Megawatt überschritten werden. Verglichen mit 2024 werden sich Deutschlands Rechenzentrumskapazitäten dann nahezu verdoppelt haben.

Regulatorik bremst, USA/China enteilen

Kontrovers wird es bei den Rahmenbedingungen. Gefordert werden verbesserte regulatorische Rahmenbedingungen, schnellere Planungs- und Genehmigungsverfahren sowie wettbewerbsfähige Strompreise. Deutsche Sonderwege durch das Energieeffizienzgesetz – etwa Vorgaben zur Energie-Verbrauchseffektivität und zum Anteil wiederverwendeter Energie – stoßen auf Kritik und sollen mit EU-Rahmen harmonisiert werden. Praxisprobleme bleiben: Kommunale Wärmeplanung, reale Abnehmer für 30- bis 40-Grad-Abwärme und die Taktung von Netzausbau lassen sich nicht herbeiregulieren. Steuerliche Anreize für Abwärme-Abnehmer könnten helfen, lösen aber weder die Topologie der Wärmenetze noch die zeitliche Kopplung von IT- und Energie-Infrastruktur. Im internationalen Vergleich setzt es derweil harte Maßstäbe: China kommt 2024 auf 38 GW IT-Anschlussleistung, die USA auf 48 GW – die zehn größten US-Rechenzentren zusammen erreichen die Größenordnung aller 2.000 deutschen Standorte. Vorhaben wie **Meta**s *Hyperion* oder KI-Cluster von **OpenAI** und **xAI** verdeutlichen, in welcher Liga dort geplant wird.

Rechenzentren: Standortentscheidungen sind Energie- und Netzfragen

Was folgt daraus für Betreiber und Entscheider? Erstens, Standortwahl ist eine Energie- und Netzfrage: Ohne frühzeitige Klärung von Strom-Kontingenten, Trafo-Kapazitäten und Einspeisepunkten drohen Verzögerungen, die jede Hardware-Roadmap ausbremsen. Zweitens, Abwärme-Nutzung wird vom Nice-to-have zum Kosten- und Lizenzfaktor – ohne realistische Abnehmer ist die beste Effizienzstrategie wenig wert. Drittens, Liquid-Cooling und Rack-Dichten jenseits von 30 kW je Rack werden zum Standard-Werkzeugkasten für KI-Lasten, auch in Colocation-Umgebungen. Viertens, Edge-Designs gehören in Ausschreibungen, wenn Latenz und lokale Datenhaltung zählen. Fünftens, Beschaffung und Architektur sollten zweigleisig fahren: kurzfristig GPU-fähige Kapazität für Pilotierung, mittelfristig eine konsolidierte Plattform, die Cloud-Anbindung und On-Prem-Souveränität vereint. Politisch bleibt entscheidend, ob Bund und Länder den Spagat zwischen Investitionssicherheit und Umweltzielen glaubhaft schaffen. Ohne starken Netzausbau und belastbare Wärme-Konzepte bleibt jeder Mega-Park nur eine Visualisierung. Oder, zugespitzt: Ohne planbare Energie- und Genehmigungs-Pfade gibt es keine Rechenzentren – und ohne Rechenzentren keine KI. ■

Weiterführende Links:

Lesen Sie eine ausführlichere Zusammenfassung der Bitkom-Studie auf speicherguide.de

www.speicherguide.de/datacenter/bitkom-ki-macht-druck-auf-deutschlands-rechenzentren-26874.html

Cybersicherheitsstudien 2025: KI, IoT & Datensouveränität im Fokus

CYBERRISIKEN FÜR UNTERNEHMEN IM ÜBERBLICK

Unternehmen stehen 2025 vor wachsenden Cyberbedrohungen durch KI, IoT und Cloud. Studien zeigen: Angriffsflächen und Schäden nehmen zu, während Prävention und Governance oft zurückbleiben. Datensouveränität und gezielte Maßnahmen werden zum Schlüsselfaktor für die IT-Sicherheit.

Michael Baumann
speicherguide.de

KI, IoT, Cloud, Technologie-Diktate und Mammut-Rechenzentren globaler Datenverarbeiter: Es scheint, als sei die Büchse der Pandora weit und unkontrolliert geöffnet. Unternehmen kämpfen damit, neue Möglichkeiten zu nutzen, während die Sicherheitsrisiken scheinbar stetig anwachsen.

Aktuelle Studien dokumentieren eine Verschärfung der Cyberbedrohungslage über alle Ebenen der Unternehmens-IT hinweg. Betroffen sind Rechenzentren, SaaS-Infrastrukturen, IoT-Umgebungen sowie klassische Endgeräte. Als kritische Faktoren identifizieren die Erhebungen KI-gestützte Angriffsmethoden, unzureichende Präventionsmaßnahmen sowie strukturelle Defizite in den Bereichen Governance und Datensouveränität.

Schadensereignisse in Unternehmen

Die **PwC**-Studie (PricewaterhouseCoopers) »*Digital Trust Insights 2026*« zeigt, dass in Deutschland 89 Prozent der befragten Unternehmen in den vergangenen drei Jahren von Datendiebstahl oder Datenmissbrauch betroffen waren. Dieser Wert liegt über dem globalen Durchschnitt von 82 Prozent. Die dokumentierten finanziellen Schäden bewegen sich in erheblichen Dimensionen: 15 Prozent der Unternehmen berichten von Verlusten zwischen 500.000 und einer Million US-Dollar, 26 Prozent geben Schäden zwischen einer und zehn Millionen US-Dollar an.

Als Reaktion planen 92 Prozent der befragten Firmen Anpassungen ihrer Sicherheitsstrategie innerhalb der nächsten zwölf Monate. Konkret wollen 55 Prozent das Cyber-Risikomanagement ausbauen, während 40 Prozent Standortwechsel für kritische Infrastrukturen prüfen. 42 Prozent passen Handels- und Betriebspolitik an, 35 Prozent erwägen den Wechsel des Sicherheitsanbieters.

KI als Angriffs- und Verteidigungsinstrument

In der PwC-Erhebung sehen sich 32 Prozent der deutschen Unternehmen unzureichend auf Angriffe im Zusammenhang mit KI und Quantencomputing vorbereitet, global sind es 26 Prozent. Weitere signifikante Risikoquellen bilden vernetzte Geräte mit 30 Prozent, Cloud-Sicherheit mit 28 Prozent und Social Engineering mit 23 Prozent.

Generative KI zeigt besonders starke Auswirkungen auf die Bedrohungslage. 67 Prozent der Sicherheitsverantwortlichen berichten von einer deutlich vergrößerten Angriffsfläche. Als zentrale Bedrohungen gelten KI-basierte Malware, Angriffe auf Lieferketten sowie Deepfakes. Parallel nut-

Bild: speicherguide.de via DALL-E

Grafik: Opentext

Zwar sind neun von zehn der Opentext-Studienteilnehmer überzeugt, sich nach einem Ransomware-Angriff erholen zu können, doch nur ein Drittel der tatsächlich betroffenen Firmen konnten ihre Daten vollständig wiederherstellen.

zen 54 Prozent der Unternehmen KI- und Machine-Learning-Werkzeuge, um den Mangel an Sicherheitsspezialisten zu kompensieren.

Trotz steigender Budgets investieren lediglich 15 Prozent der Firmen in systematische Präventionsprogramme. Rund 80 Prozent erhöhen zwar ihre Ausgaben für Cybersicherheit, konzentrieren sich dabei jedoch auf Netzwerksicherheit, Zero-Trust-Modelle, KI-Funktionen und Cloud-Security. Frühwarnsysteme und risikobasierte Planung bleiben vergleichsweise unterentwickelt.

Ransomware-Resilienz: Diskrepanz zwischen Einschätzung und Realität

Die **OpenText**-Studie »*Cybersecurity 2025 Global Ransomware Survey*« dokumentiert eine erhebliche Diskrepanz zwischen Selbsteinschätzung und tatsächlicher Wiederherstellungsfähigkeit. In Deutschland fühlen sich 88 Prozent der befragten Unternehmen gut gegen Ransomware gerüstet, neun von zehn gehen von einer erfolgreichen Wiederherstellung nach einem Angriff aus.

Die realen Wiederherstellungsraten fallen deutlich niedriger aus. Nur 30 Prozent der tatsächlich betroffenen Organisationen konnten ihre Daten vollständig wiederherstellen. Zwei von fünf Unternehmen wurden 2024/25 Opfer mindestens eines Ransomware-Angriffs, mehr als die Hälfte davon mehrfach. Etwa 14 Prozent der betroffenen Organisationen zahlten Lösegeld, bei der Hälfte dieser Fälle lagen die Zahlungen über 250.000 US-Dollar.

Im Kontext generativer KI zeigt sich ein weiteres Governance-Defizit. 90 Prozent der Unternehmen erlauben ihren Mitarbeitenden den Einsatz entsprechender Tools, jedoch verfügen nur 32 Prozent über verbindliche Richtlinien.

SaaS: Hohe Komplexität, unklare Verantwortlichkeiten

Der **HYCU**-Report »*State of SaaS Resilience 2025*« beleuchtet die Risiken im SaaS-Umfeld. Die befragten Unternehmen nutzten im Durchschnitt 139 SaaS-Anwendungen, bei Organisationen mit vorangegangenen Sicherheitsvorfällen steigt dieser Wert auf 159. 65 Prozent verzeichneten im letzten Jahr mindestens eine SaaS-bezogene Sicherheitsverletzung.

Die wirtschaftlichen Auswirkungen sind erheblich. Die durchschnittlichen täglichen Kosten von SaaS-Downtimes werden mit 405.770 US-Dollar beziffert, die Wiederherstellung dauert im Mittel fünf Arbeitstage. Daraus ergibt sich ein durchschnittlicher direkter Schaden von etwa 2,3 Millionen US-Dollar pro Vorfall, ohne immaterielle Folgen wie Reputationsverlust.

Strukturelle Schwächen zeigen sich insbesondere bei Zuständigkeiten und Schutzkonzepten. 43 Prozent der Teilnehmenden geben an, dass niemand klar für SaaS-Datenresilienz verantwortlich ist. In vielen Fällen kontrolliert die IT-Abteilung lediglich etwa 56 Prozent des SaaS-Stacks, vollständige Kontrolle bildet die Ausnahme.

66 Prozent der Unternehmen verlassen sich primär auf die Anbieter und sehen diese in der Hauptverantwortung für Datensicherung. Die Studie zeigt jedoch, dass 87 Prozent mindestens einen SaaS-Typ ohne ausreichenden Schutz einsetzen. Nur 30 Prozent nutzen richtlinienbasierte Backups, 26 Prozent externe Aufbewahrung und 25 Prozent regelmäßige Recovery-Tests.

IoT & hybride Umgebungen als Angriffsvektor

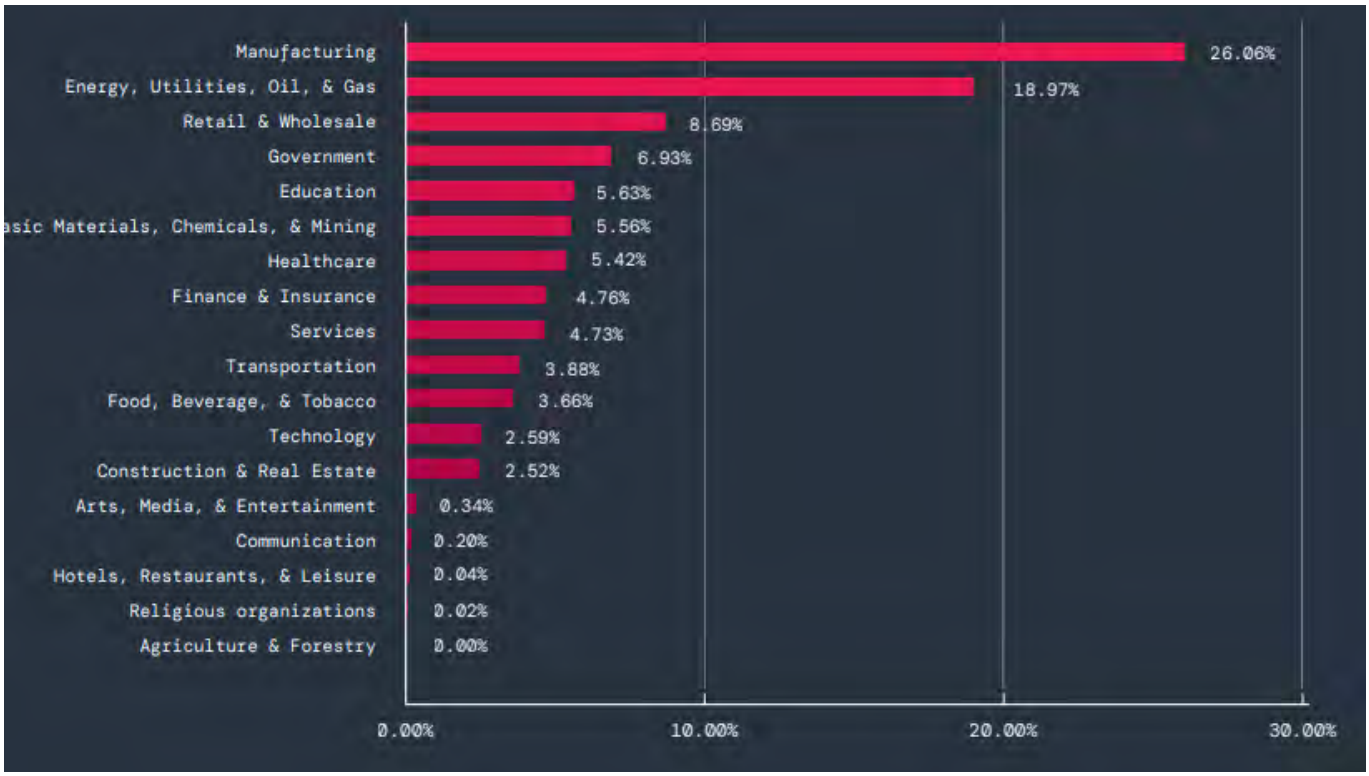
Der **Zscaler**-Report »*ThreatLabz 2025 Mobile, IoT and OT Threat Report*« dokumentiert einen Anstieg von Malware um 67 Prozent im Jahresvergleich. Besonders betroffen sind hybride Arbeitsumgebungen und kritische Industrien. Im IoT-Segment entfallen jeweils 20,2 Prozent der beobachteten Angriffe auf Fertigung und Transport.

Die **Bitdefender/Netgear**-Analyse »*2025 IoT Security Landscape Report*« ergänzt die Perspektive auf vernetzte Unternehmensumgebungen. Ein durchschnittlicher Haushalt mit Home-Office-Anbindung verfügt über 22 vernetzte Endpunkte und ist im Mittel fast 29 Angriffen pro Tag ausgesetzt. Dies entspricht nahezu einer Verdreifachung gegenüber dem Vorjahr mit zehn Angriffen.

Schatten-KI und Governance-Defizite

Eine **Bitkom Research**-Umfrage vom Oktober 2025 zur Nutzung generativer

Die am häufigsten angegriffenen Branchen



Grafik: Zscaler

Das produzierende Gewerbe steht mit Abstand am stärksten im Fokus von Cyberkriminellen.

KI in Unternehmen dokumentiert erhebliche Governance-Lücken. Vier von zehn Unternehmen gehen davon aus, dass Mitarbeitende private KI-Zugänge wie ChatGPT oder andere generative Dienste im Arbeitskontext verwenden. In acht Prozent der Unternehmen ist dies weit verbreitet, in 17 Prozent treten Einzelfälle auf. Weitere 17 Prozent vermuten die Nutzung ohne belastbare Erkenntnisse.

Während 26 Prozent der Unternehmen einen offiziellen Zugang zu generativer KI bereitstellen, planen 17 Prozent entsprechende Angebote. 30 Prozent können sich dies vorstellen, 14 Prozent schließen es aus. Governance-Regelwerke sind nicht flächendeckend vorhanden: 23 Prozent der Unternehmen haben Richtlinien für den Einsatz von KI-Tools definiert, 31 Prozent planen diese. 16 Prozent wollen auch künftig darauf verzichten, 24 Prozent haben sich bislang nicht mit dem Thema beschäftigt.

Datensouveränität als Auswahlkriterium

Eine von **Ionos** beauftragte Erhebung unter etwa 4.500 Entscheidungsträgern in europäischen KMU zeigt, dass digitale Souveränität zu einem zentralen Auswahlkriterium für IT-Dienstleister geworden ist. Mehr als vier von fünf Befragten bevorzugen Anbieter, die vollständige Kontrolle über Unternehmens- und Kundendaten gewährleisten und diese vor dem Zugriff ausländischer Behörden schützen. In Deutschland stufen 89 Prozent Datenhoheit als essenziell ein, Spanien, Frankreich und Großbritannien folgen mit 87 Prozent. Darüber hinaus fordern viele Unternehmen Unabhängigkeit von nicht-europäischen politischen Entscheidungen sowie transparente Rechenzentrumsstandorte mit nachweislich hohem Sicherheitsniveau. Dies deutet auf eine wachsende Bedeutung von Multi-Cloud-Strategien, Exit-Szenarien und europäischen EU-Only-Modellen mit klarer Governance hin.

Strukturelle Herausforderungen

Die vorliegenden Studien zeigen, dass Cyberrisiken 2025 entlang der gesamten IT-Wertschöpfungskette zunehmen. Schadensereignisse treten häufig auf und verursachen teilweise erhebliche direkte Kosten. KI und Automatisierung verstärken sowohl Angriffs- als auch Verteidigungsmechanismen, während Prävention, Zuständigkeiten, Governance und Datensouveränität vielfach zurückbleiben. ■

Weiterführende Infos auf speicherguide.de:

- PwC-Studie: Datenklau und neue Cyberrisiken durch KI und Quanten
- Opentext-Studie: Falsche Ransomware-Zuversicht in Deutschland
- Bitdefender-/Netgear-Studie: IoT-Angriffe nahezu verdreifacht
- Hycu-Studie: SaaS boomt – die Datenresilienz nicht
- KMU fordern Datenhoheit: Ionos-Studie zu digitaler Souveränität