storage-magazin.de

Eine Publikation von speicherguide.de

powered by it-daily.net

1 | 2024

- **TREND**
  Storage immer komplexer
- **SICHERHEIT**
  Bedrohung durch Cyberprofis
- **STRATEGIE**
  Skepsis gegenüber Cloud

35 Seiten geballtes Storage-Wissen

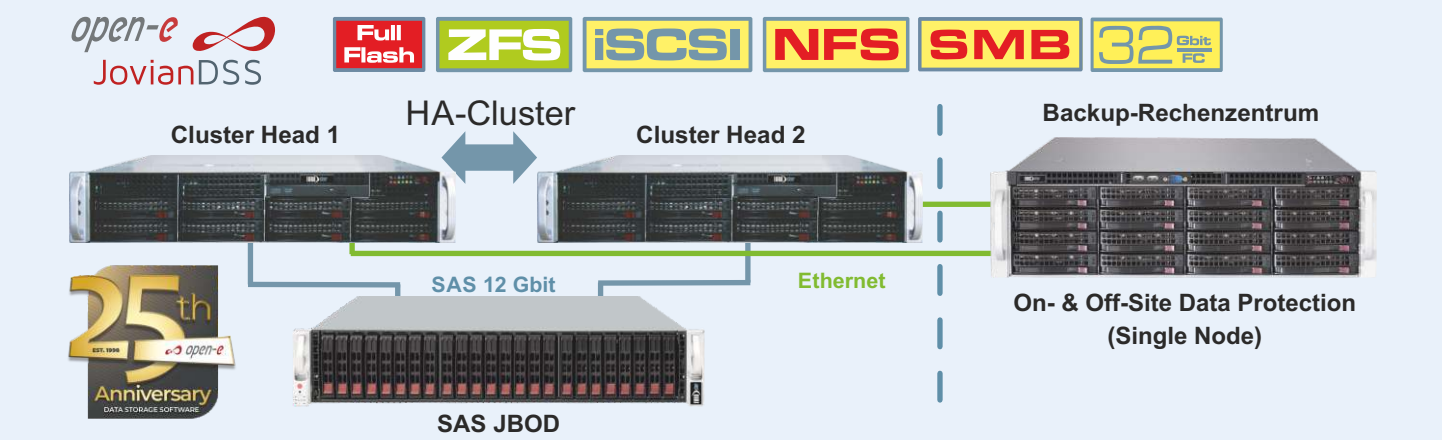
Einkaufsführer Storage 2024

Grafik: Dall-E (KI)

Schlanke Datensicherung für KMU

Open-E JovianDSS ZFS Cluster mit neuen Features

Storage Cluster mit **Open-E JovianDSS** sichern die Verfügbarkeit der Daten sowohl durch die Active/Active Redundanz der Clusterknoten als auch durch die Fehlertoleranz des **ZFS** Filesystems. Mit dem neuen Release, das derzeit in Vorbereitung ist, werden außer dem ZIL- und Readcache auch sogenannte **„ZFS Special Devices“** unterstützt. Das ist ein SSD Schreibcache für Metadaten und kleinere Datenpakete, wodurch eine Performancesteigerung erzielt wird. Auch bei der snapshotbasierten Sicherung der Daten in ein ODP System (**On- & Off-Site Data Protection**) bringt die neue Version Vorteile: Komprimierte Daten werden zur Synchronisation nicht mehr entpackt, sondern direkt als „raw data“ übermittelt, was vor allem bei geringer Netzwerk-Bandbreite den Durchsatz verbessert.



ES-8700JDSS Cluster mit iSCSI/NAS zu den Clients + ODP Schutz vor Ransomware

zwei Cluster Knoten, active/active, je 4 x 10 GbE Hostanbindung + 24-Slot Shared Storage SAS JBOD, teilbestückt: 12 x 3,84 TB SAS SSD (2 vdevs RAID-Z2, 25,2 TiB), inkl. Open-E JovianDSS Lizenzen, Preis zzgl. Installation

inkl. MwSt. **€ 32.011,-** exkl. MwSt. **€ 26.900,-**

16-Slot Server System, On- & Off-Site Data Protection System für den Cluster, teilbestückt mit 9 x 12 TB Nearline SAS Disks (1 vdev RAID-Z3, 59 TiB usable), inkl. Open-E JovianDSS Lizenzen

inkl. MwSt. **€ 13.673,10** exkl. MwSt. **€ 11.490,-**

ES-8700JDSS Cluster und Backup System

- 2 HE Cluster Knoten mit zwei Intel Xeon 4215R Prozessoren, 8 Core, 3.2 GHz auf X11 Board, 192 GB RAM,
- 2 x 10 GbE RJ45 (opt. SFP+) für Interconnect + 2 x 10 GbE (SFP+) zu den Clients (optional bis 100 GbE und FC Ports)
- JBOD: 12 Gbit SAS 24, 2 HE (opt. mehrere JBODs)
- On- & Off-Site Data Protection: 3 HE 16-Slot Server Intel Xeon 6134 Prozessor, 8 Core, 3.2 GHz auf X11 Board, 128 GB RAM, 2 x 10 GbE RJ45, opt. weitere Ports bis 100 GbE
- IPMI 2.0 RJ45 Port für Überwachung / Remote Management
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

Als zusätzlicher Schutz lassen sich die SSDs zweier JBODs untereinander spiegeln. Mit 3 JBODs können auch RAID-Z2 vdevs aus je 2 SSDs pro Box realisiert werden.

Open-E JovianDSS iSCSI/NAS/FC Software:

- ZFS 2.0 Filesystem für maximale Datenintegrität
- Schutz vor „Stealth Errors“ durch Check-Summen-Prüfung und Disk-Scrubbing
- Plattenredundanz durch Mirror, RAID-Z, -Z2, -Z3 (entspricht RAID 1, 5, 6 und dreifacher Parity)
- SSDs zur I/O-Beschleunigung (Read/Write-Cache)
- konfigurierbar als shared Storage active/active Cluster
- praktisch unbegrenzte Snapshots und mountbare Snapshot-Volume-Clones ohne Performanceverlust
- iSCSI, NFS und CIFS/SMB Volumes, opt. Fibre Channel
- Thin- und Thick-Provisioning
- LZ4 Datenkompression und inline Deduplikation
- On- & Off-Site Data Protection zur Datensicherung auf weiteres System, Reaktivierung in wenigen Minuten
- intuitive Web-GUI für einfaches Management
- 3 Jahre Open-E Standard Support (E-Mail und Telefon), optional erweiterte Open-E Services
- Installation und Konfiguration vor Ort / remote durch EUROstor (berechnet nach Aufwand)

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, Scale-Out Clustern, Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die Server-Virtualisierung. Registrieren Sie sich einfach unter www.EUROstor.com/Newsletter, oder rufen Sie uns an!

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

Preisänderung, Druckfehler und Irrtum vorbehalten.

Editorial

Karl Fröhlich
Chefredakteur
speicherguide.de

RANSOMWARE BETRIFFT NICHT NUR TECHNIK

So schnell kann es gehen, letztes Jahr berichtet ich an dieser Stelle von vollen Auftragsbüchern. Wobei damals schon inflationsbedingte Kaufaufschübe im Raum standen. Nun, ein Jahr später ist es genau so gekommen, Projekte werden aufgeschoben. Oft auf unbestimmte Zeit. Selbst an Sicherheitsmaßnahmen wird gespart. Wie wir hören, wurden selbst einige große Security-Projekte nicht umgesetzt. Zu unsicher ist die Lage ...

Hinzukommt der Personalmangel, auch nicht neu, aber wer soll die IT der Zukunft planen und umsetzen? Da genügt oft schon ein Kollege im Krankenstand und das Tagesgeschäft frisst alle hochtrabenden Pläne auf. Das ist bei uns nicht anders. Wir würden gerne noch mehr rausgehen und mit unseren Leser sprechen, meist bleibt es bei den üblichen Herstellerthemen.

Erschwerend kommt hinzu, dass Ransomware nicht nur die IT und den Datenzugriff lahmlegt, sondern auch massive Auswirkungen auf die Kollegen hat. Ein befreundeter IT-Leiter hat mit seinen Leuten einen Cyberangriff durchgestanden. Sieben Wochen hat es gedauert, bis alles wieder halbwegs »up and running« war. Nun hatten sie Glück, weil die Geschäftsleitung umsichtig gehandelt und keinen Druck ausgeübt hat. Dies ist oft genug nicht der Fall. Laut Statistik werden drei von seinen Mitarbeitern an Burnout erkranken. »Das musst Du Dir mal vorstellen, in Deinen Artikeln liest sich sowas ganz handsam, aber jetzt sind Leute betroffen, die ich kenne. Bei uns haben alle mitangepackt, zum Teil rund um die Uhr. Einige musste ich zwingen nach Hause zu gehen und die Füße hochzulegen.«

Ein entscheidender Faktor bei der Bekämpfung eines Ransomware-Angriffs, ist auch seine Leute zu versorgen, damit sie nicht ausbrennen. Wir schreiben ja auch immer wieder, dass man sich vorbereiten soll. Ich glaube, auf einiges kann man sich nur schwer vorbereiten. Ein Schritt nach vorne wäre, wenn es bereits eine Struktur für die ersten Maßnahmen gäbe. Auf der Storage2day habe ich mit einem Sicherheitsexperten gesprochen und der meinte, Schulungen müssen gar nicht das ganze Unternehmen betreffen, sondern es wäre besser diese abteilungsweise aufzuteilen. Beispielsweise für alle, die in der Administration zuständig sein werden, eine Nachrichtenkette aufzubauen, die alle Kollegen informieren, dass sie eventuell nicht zu kommen brauchen. In der Regel sei es so, dass die Leute beim ersten Mal nach einer Stunden verzweifelt und fertig wären. Beim zweiten Versuch würde es fast immer bedeutend besser laufen. Übung macht den Meister, in allen Bereichen.

Lesen Sie in dieser Ausgabe mehr über Strategien, Trends und Lösungen in den Bereichen Datenspeicherung und Storage-Infrastrukturen.

Karl Fröhlich
Chefredakteur, speicherguide.de

Grafik: Dall-E (KI)

Lieferschwierigkeiten und politische Lage verunsichern den Storage-Markt

NEUES LEVEL: STORAGE-ANFORDERUNGEN IMMER KOMPLEXER

SEITE 5

2023 ist der Storage-Markt geprägt von Verunsicherung. Wachsende Datenmengen und steigende Kosten definieren den Markt neu. Gleichzeitig erschwert die weltpolitischen Lage, die Entscheidungsfindung in den Unternehmen.

Cyberabwehr 2023: KMUs im Fokus von Ransomware

DATEN IN GEFAHR: CYBERKRIMINELLE IMMER PROFESSIONELLER

Grafik: Dall-E (KI)

SEITE 18

Container: skalierbar, flexibel und robust, aber auch ein Sicherheitsrisiko

BEI DER CONTAINER-NUTZUNG DIE SICHERHEIT NICHT VERGESSEN

Grafik: Dall-E (KI)

SEITE 26

Editorial 3

Inhalt/Impressum 4

Datenspeicherung

Neues Level: Storage-Anforderungen immer komplexer 5

Advertorial

Digitale Infrastruktur aus dem Rechenzentrum mit Open-E JovianDSS 10

Aktives WORM-Archiv verschlankt Datensicherung 12

Datensicherung für kleinere IT-Umgebungen 14

Datenspeicherung

Übersicht Storage-Anbieter 16

Cybersicherheit

Daten in Gefahr: Cyberkriminelle immer professioneller 18

Infrastruktur

IT-Manager bleiben bei der Cloud skeptisch 22

Bei der Container-Nutzung die Sicherheit nicht vergessen 26

Datenspeicherung

Primärspeicher: Kern der IT-Infrastruktur 30

Management

IT-Fachkräftemangel: Effizienz und Recruiting als Schlüssel 34

Übersicht **Storage-Anbieter**

SEITE 16

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, Peter Marwan

Schlussredaktion:
Brigitte Scholz

Titelbild:
Dall-E (KI)

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

Karen Reetz
Media Consulting
Tel: 08121 / 977594
E-Mail: reetz@it-verlag.de

Webkonzeption und Technik:
IT Verlag GmbH
Ludwig-Ganghofer-Str. 51
Otterfing 83624
E-Mail: webmaster@speicherguide.de

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

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

Lieferschwierigkeiten und politische Lage verunsichern den Storage-Markt

NEUES LEVEL: STORAGE-ANFORDERUNGEN IMMER KOMPLEXER

Michael Baumann
speicherguide.de

Karl Fröhlich
speicherguide.de

2023 ist der Storage-Markt geprägt von Verunsicherung. Wachsende Datenmengen und steigende Kosten definieren den Markt neu. Gleichzeitig erschwert die weltpolitischen Lage, die Entscheidungsfindung in den Unternehmen, die derzeit nicht unbedingt technikbasiert ist. Die Anforderungen erreichen ein neues Level.

Im Storage-Umfeld sehen sich die Leser von *speicherguide.de* vor allem mit zwei Herausforderungen konfrontiert: dem Datenwachstum und den Kosten. In unserer Leserumfrage ist der stetig größer werdende Speicherbedarf bei rund 58 Prozent der Befragten ein großes Thema.

64 Prozent geben an, bis 500 TByte Kapazität für Sekundärdaten vorzuhalten. Zwölf Prozent verwenden zu diesen Zwecken bis zu ein sowie weitere zehn Prozent bis zu 10 PByte. Insgesamt 16 Prozent der Unternehmen liegen über dieser Marke und davon eine Spitzengruppe von zwei Prozent, die mit über 200 PByte konfrontiert sind.

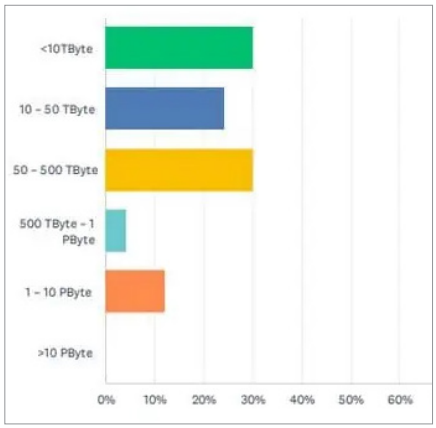
Für Primärdaten benötigen Unternehmen deutlich weniger Speicherkapazität: 54 Prozente kommen mit 50 TByte zurecht. Für die *speicherguide.de*-Redaktion ist dies auch ein Indiz, dass viele kleine und mittelständische Unternehmen (KMU) zu den Umfrageteilnehmern zählen. 39 Prozent bewe-

Grafik: Dall-E (KI)

gen sich in einem mittleren Segment bis 1 PByte. Zwölf Prozent siedeln sich im Bereich über 1 PByte an und damit, je nach Branche, in einem Bereich, der auf größeren Mittelstand und Enterprise hinweisen könnte.

IDC erwartet, dass im Jahr 2023 mehr als 129 ZByte an Daten generiert werden, die sich bis 2027 auf über 291 ZByte mehr als verdoppeln sollen. Dies entspricht einer durchschnittlichen jährlichen Wachstumsrate von 22,4 Prozent zwischen 2022 und 2027.

2019 erzeugte die Weltbevölkerung noch 43 ZByte. Vor drei Jahren erklärten IDC-Manager gegenüber *speicherguide.de*: »Für 2024 rechnen wir jetzt mit 143 ZByte, das ist ein jährliches Plus 26 Prozent.«



Quelle: it-daily.net/speicherguide.de

Wie viel Speicherkapazität benötigen Sie zum Speichern Ihrer Primärdaten?

Kosten und Lieferfähigkeit

Knapp 46 Prozent unserer Leser kämpfen mit hohen Investitionskosten, trotz Abo- und Miet-Modellen, um die Ausgaben in Richtung Betrieb versus Investition zu lenken (OPEX versus CAPEX). Noch mehr überrascht, dass rund 23 Prozent steigende Hardware-Preise bemängeln. Diese Angabe kann eigentlich bei der Betrachtung von Kosten pro GByte sämtlicher Datenträger (HDD, SSD, Tape) eigentlich kaum bestätigt werden.

Die Beschaffung ist ebenfalls ein Thema, dass nicht immer reibungslos von statten geht: Ein Viertel geben Lieferproblem beim Hardware-Kauf an.

»2024 erwarten wir eine weitere Modernisierungswelle. Flash und auch Energiemanagement gewinnen an Bedeutung.«

Thomas Muggendobler, Thomas-Krenn

Bild: Thomas-Krenn

»Die Gesamtproblematik ist zwar etwas abgeflacht, dennoch zählt weiterhin vielfach die Lieferfähigkeit«, erklärt **Thomas Muggendobler**, Senior Product Manager Datacenter Solutions bei **Thomas-Krenn**, gegenüber *speicherguide.de*. »Das gilt vor allem wegen der zu erwartenden Preissteigerungen 2024 im Flash-Bereich, die sich auf RAM und Datenträger auswirken dürften. Damit sind auch hohe Erwartungen an die Angebotsgültigkeit verbunden, hier sind wir so weit wie möglich entgegenkommend. Die aktuellen geopolitischen Krisen spielen da natürlich auch eine Rolle.«

Kaufverhalten: Unsicherheit im Markt

Die weltpolitische Lage sorgt definitiv für Versunischerung. Dies sieht auch **Albrecht Hestermann**, Leiter Vertrieb, Marketing & Produktmarketing bei **actidata Storage Systems**: »Generell lässt insbesondere für viele Unternehmen im SMB-Markt konsternieren, dass eine große Unsicherheit hinsichtlich der wirtschaftlichen Zukunftsentwicklung besteht. Automobil-Zulieferer beispielsweise, die aktuell in den Wirtschaftsräumen Ostwestfalen und Stuttgart mit Investitionen eher vorsichtig umgehen. Für uns bedeutet diese Situation, noch enger mit den Administratoren zusammenzuarbeiten um letztlich maßgeschneiderte Lösungen anzubieten, die hinsichtlich Preis und Leistung zu engen Budgets passen.«

Vertrauen ist auch ein Punkt, der zum Punkt Kompatibilität passt. Mit der Diversifizierung von Lösungen und Technologien leiden nach den Leser-Angaben 35,42 Prozent an der Inkompatibilität von Systemen und Komponenten. Auch dies eine Aussage, die keine Marketing-Abteilung bewährter Hersteller unterschreiben würde. Dort haben die Anbieter nun die Aufgabe, sich mit ihrer Klientel auseinanderzusetzen.

Insgesamt deckt sich das, mit Aussagen, die wir aus der Branche hören. Viele Unternehmen schieben Investitionen und Projekte auf. Das Kaufverhalten ist mehr als zögerlich. Unternehmen kaufen derzeit nur, was unbedingt benötigt wird. Dies hatte sich bereits im erste Halbjahr 2023 angedeutet. Marktbeobachter hatten noch erwartet, dass es im zweiten Halbjahr besser würde, dies ist bisher nicht der Fall. Vielmehr haben die meisten Storage-Anbieter auch das Weihnachtsgeschäft bereits abgeschrieben. Einen, eigentlich traditionell starken Jahresendspurt, wird es heuer nicht geben.

Da sich Lage in der Weltmarkt auf absehbare Zeit nicht ändern wird, muss die IT- und Storage-Branche, mit einem weiteren Abschwung rechnen. Bestenfalls bewegt sich der Markt seitwärts. Traditionell bedeutete dies in der Vergangenheit bisher immer, dass Anbieter, die ihre Bilanz öffentlich vorweisen müssen, in Ausschreibungen mit sehr aggressiven Preisen agierten.

Die Marktforscher von **Context** hatten es schon geahnt und ein eher pessimistisches Prognoseszenario vorhergesagt. Bereits im Mai hieß es, Storage-Anbieter sollten sich im drit-

»Im SMB-Markt besteht eine große Unsicherheit hinsichtlich der wirtschaftlichen Zukunftsentwicklung.«

Albrecht Hestermann, Actidata

Bild: Actidata

ten und vierten Quartal auf einen Umsatzrückgang von knapp unter sechs Prozent einstellen. Das Gesamtjahr fiele dann mit einem Plus von einem Prozent äußerst unbefriedigend aus.

Vorhersagen für die strategische Planung

Die weltweiten IT-Gesamtausgaben sehen Analysten für das laufende Jahr noch ein Plus. Gartner erwartet gegenüber 2022 einen Anstieg um 5,1 Prozent auf insgesamt 4,6 Billionen US-Dollar. **John-David Lovelock**, Distinguished VP Analyst bei Gartner. »CEOs und CFOs erhöhen die Ausgaben für digitale Geschäftsinitiativen, statt die IT-Budgets zu kürzen. Wirtschaftliche Turbulenzen werden den Kontext für Technologieinvestitionen verändern, indem sie die Ausgaben in einigen Bereichen erhöhen und den Rückgang in anderen beschleunigen.« Das Gesamtniveau der Technologieausgaben von Unternehmen sollen sie allerdings nicht wesentlich beeinflussen.

Neue Aufwendungen verlagern sich weiterhin auf Cloud-Optionen. Dies verdeutliche laut Gartner das für 2023 prognostizierte Wachstum der Software-Ausgaben von 11,3 Prozent. On-Premises habe trotzdem weiter bestand. Es seien genügend Mittel für den Betrieb und Erhalt von Rechenzentren vorhanden.

Storage-Infrastruktur als Bereitstellungsplattform

Bis 2026 sollen Gartner zufolge SLA-Garantien auf der Basis von Speicherverbrauchs-Plattformen mehr als 50 Prozent der herkömmlichen Aktivitäten in den Bereichen IT-Kapazitätsmanagement, -budgetierung, -bewertung, -beschaffung und -erfüllung vor Ort ersetzen.

2023 steht die Branche noch bei unter zehn Prozent. 2023 verwenden Firmen rund 85 Prozent ihres Budgets Storage-Infrastrukturen für Hardware-Management und IT-Support-Fähigkeiten auf. Bis 2027 sollen es nur noch zirka 30 Prozent sein. Bis 2028 werden verbrauchsbasierte STaaS mehr als 35 Prozent der Investitionsausgaben (Capex) von Unternehmen für Speicher ersetzen, im Vergleich zu weniger als zehn Prozent im Jahr 2023.

Gartner erwartet, dass der Markt für Primärspeicher in eine Phase beschleunigter Innovation eintritt. Unternehmen gehen demzufolge weg von der traditionellen Investitionsfinanzierung und Budgetierung hin zu einer hybriden Plattformstrategie. Dies soll auch für On-Premises eine Cloud-Betriebsmodell enthalten und neue Methoden zur Finanzierung und Verwaltung von Speicher-Ressourcen umfassen. Die Fortschritte der Anbieter bei den Plattformfunktionen, der Daten- und Cybersicherheit und den neuen Speicher-OS-Architekturen bieten Verantwortlichen für Infrastruktur und Operations (I&O) SLAs, die auf die Ergebnisse des IT-Betriebsmodells ausgerichtet sein sollen. Die grundlegendste Frage, mit der sich I&O-Führungskräfte konfrontiert sehen, ist, wie sie Zugang zu Cloud-ähnlichen Vorteilen erhalten und gleichzeitig ein hohes Maß an Ausfallsicherheit und Kontrolle, über die auf zentralen Diensten basierende IT-Betriebsinfrastruktur bewahren können.

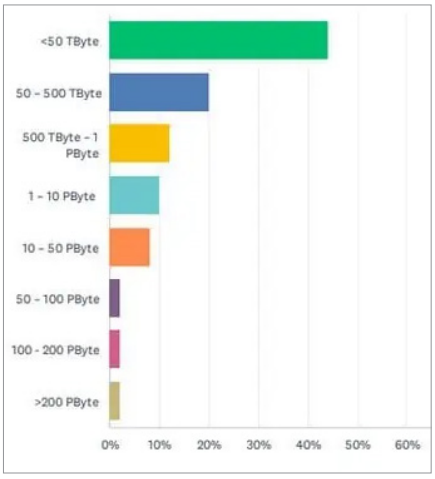
IT-Infrastrukturen im Wandel

Fujitsu zufolge sind leistungsfähige und smarte IT-Infrastrukturen heute unbedingte Voraussetzung für die Zukunftsfähigkeit von Organisationen und Unternehmen. Der Hersteller spricht hier auch von der nächsten Generation von Rechenzentren. »Maßgebliche Aspekte sind dabei entsprechend zukunftsfähige Infrastrukturen, aber auch Edge- und Quanten-Computing – und vor allem mehr Nachhaltigkeit durch eine immer höhere Digitalisierung aller Bereiche«, erklärt **Santosh Wadwa**, Head of Product Channel Sales bei Fujitsu.

»Wirklich interessante Konzepte sehen wir auch beim Edge-Computing«, ergänzt Thomas-Krenn Manager Muggendobler. »Noch nicht so viele, aber innovative und immer mehr. Vom Imker bis zum großen Automobil- oder Landmaschinenhersteller, die Anfragen sind meist sehr individuell.«

Infrastruktur muss helfen die Daten aufzubereiten

Definitiv im Trend, datenintensive Workloads und KI (Künstliche Intelligenz) sowie Machine-Learning (ML). Um hier Schritt zu halten, werden die meisten Unternehmen nicht um neue Investments herumkommen. Neben der Speicherkapazität ist eine hohe Performance entscheidend. Daten



Quelle: it-daily.net/speicherguide.de

In der Praxis fallen rund 80 Prozent der gespeicherten Informationen in den Bereich Sekundärdaten.

»Tape ist nicht das nachhaltigste Medium, wenn es nur herumliegt, bringt es keine Wertschöpfung.«

Hannes Heckel, Fast LTA

Bild: Fast LTA

müssen sich schnell lesen und schreiben lassen, um effiziente KI-Operationen zu ermöglichen.

Mit der Zunahme der Datenmenge steigt auch die Bedeutung von Datensicherheit und Datenschutz. Speichersysteme müssen robuste Sicherheitsfunktionen bieten, um Daten vor unbefugtem Zugriff und Cyberangriffen zu schützen. Ebenfalls Teil der Strategie, ein effizientes Datenmanagement.

Das heißt, Tools für Datenanalytik, automatisierte Datenklassifizierung und intelligentes Datenmanagement sind erforderlich, um den Überblick über große Datenmengen zu behalten und deren Wert zu maximieren.

Dem pflichtet **Denis Kennelly**, General Manager bei **IBM Storage**, bei, anlässlich der Vorstellung von neuen auf KI abgestimmten Storage-Systemen: »Um den wirtschaftlichen Nutzen sowohl von Basismodellen als auch von traditionellen KI-Modellen zu nutzen, müssen sich Unternehmen auf die Daten konzentrieren. Das heißt, seine aktuellen Kapazitäts- und Wachstumsprognosen zu kennen, wo sich die Daten befinden, wie sie gesichert und zugänglich sind und wie künftige Investitionen in Datenspeicher optimiert werden können. Das Potenzial der neuen KI-Ära von heute lässt sich meiner Meinung nach nur voll ausschöpfen, wenn Unternehmen eine Strategie haben, Daten aus mehreren Quellen nahezu in Echtzeit zusammenzuführen, ohne zahlreiche Kopien von Daten zu erstellen und konstante Iterationen der Datenaufnahme zu durchlaufen.«

KI hilft bei Compliance und Datenschutz

»Mehr noch als der Hype um generative KI beschäftigt unsere Kunden aktuell die Frage nach Einsatzszenarien, die bereits heute einen konkreten Mehrwert liefern können«, ergänzt **Mark Molyneux**, EMEA CTO bei **Cohesity**. Als spannendes KI-Beispiel nennt er den Bereich Compliance und Datenschutz. Die internationale Wirtschaftskanzlei **DLA Piper** hat kürzlich eine Studie zu den Bußgeldern wegen Verstößen gegen die DSGVO in der Europäischen Union veröffentlicht, nach der die europäischen Datenschutzbehörden im Jahr 2022 Bußgelder in Höhe von 1,64 Milliarden Euro verhängt haben. Gegenüber dem Vorjahr entspricht dies einem Anstieg von 50 Prozent.

»Die meisten Unternehmen haben Berge von Informationen angehäuft, von deren Inhalten sie wenig oder nichts wissen«, erklärt Molyneux. »KI und maschinelles Lernen können hier massiv helfen und durch die automatische Klassifizierung von Unternehmensdaten eines der komplexesten Probleme entschärfen. Vordefinierte Filter fischen sofort Compliance-relevante Daten wie Kreditkarten oder andere persönliche Daten aus dem Datenpool und markieren sie. Sobald diese KI die Daten freigibt, entwickelt sie eine unternehmensbezogene Sprache, einen Unternehmensdialekt. Und je länger sie arbeitet und je mehr Unternehmensdaten sie untersucht, desto genauer werden ihre Ergebnisse. Unternehmen werden so nicht nur in die Lage versetzt, gesuchte Daten schnell und vollständig zu identifizieren, sondern auch automatisiert veraltete, verwaiste und redundante Daten zu markieren, die gelöscht werden könnten. So werden nicht nur die Anforderungen der DSGVO erfüllt, sondern auch die Datenmenge reduziert und so Kosten reduziert.«

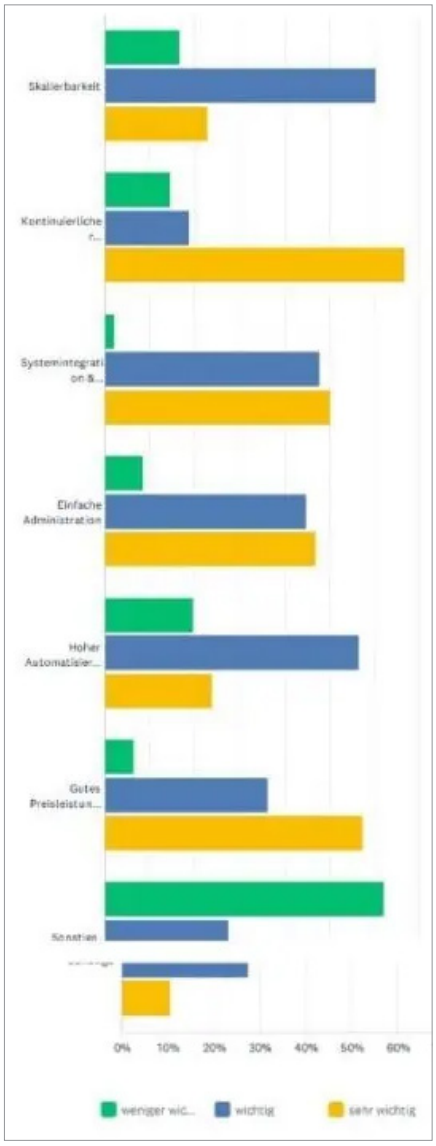
Datenmanagement bis ins Archiv

Seine Daten zu kennen, bedeutet auch, sie auf einem passenden Speichermedium abzulegen. Die Storage-Tiering genannte Optimierung basiert grundlegend auf der Nutzungshäufigkeit und Wichtigkeit der Informationen. Jedes Tier nutzt unterschiedliche Speichertechnologien, die jeweils einen Kompromiss zwischen Kosten, Zugriffsgeschwindigkeit und Kapazität darstellen.

Aufgrund des Datenwachstums sollten auch Backup und Archivierung in die Datenmanagement-Strategie miteinbezogen werden. Um vor den Folgen eines Ransomware-Angriffs zu schützen, sollten die Backups möglichst oft stattfinden und lang zurückreichend. Das heißt, in der Praxis oft, man behält die Daten über ein halbes Jahr auf Festplatte, bevor sie auf ein Medium wechseln, welches eventuell keinen sofortigen Zugriff darauf gewährt.

Um das Backup zu entlasten empfiehlt **Hannes Heckel**, Leiter Marketing bei **FAST LTA**, zusätzlich ein aktives Archiv. Anstelle von Tape, dem klassischen Archivmedium, bieten Disk-Arrays einige Vorteile: Die Daten bleiben im schnellen und nahezu unmittelbaren Zugriff. Dadurch sollen sich leichter Synergien zwischen alten und neuen Datenbeständen schaffen lassen, um beispielsweise mit Data-Analytics und Business-Intelligence-Tool schneller Erkenntnissen zu erzielen.

Backup-Lösungen sind relativ komplex geworden. Mit der Bedeutung von Daten nimmt aber auch die Bedrohungslage stetig zu. »Es gilt, sich auf allen Ebenen vor Kontrollverlust zu schützen«, rät Heckel. »Da Cyberattacken inzwischen fast immer zuerst auf



Quelle: it-daily.net/speicherguide.de

Den Höchstwert für die Einstufung als »sehr wichtig« erreicht die Kategorie »Kontinuierlicher Betrieb und Hochverfügbarkeit«, vor dem Preis-/Leistungs-Verhältnis und »Systemintegration und Kompatibilität«.

Backups zielen, reicht die einfache Datensicherung nicht mehr aus.« Vielmehr müssen mit Air-Gap und Immutability Technologien eingesetzt werden, um Backups vor Manipulation und Löschen zu schützen.

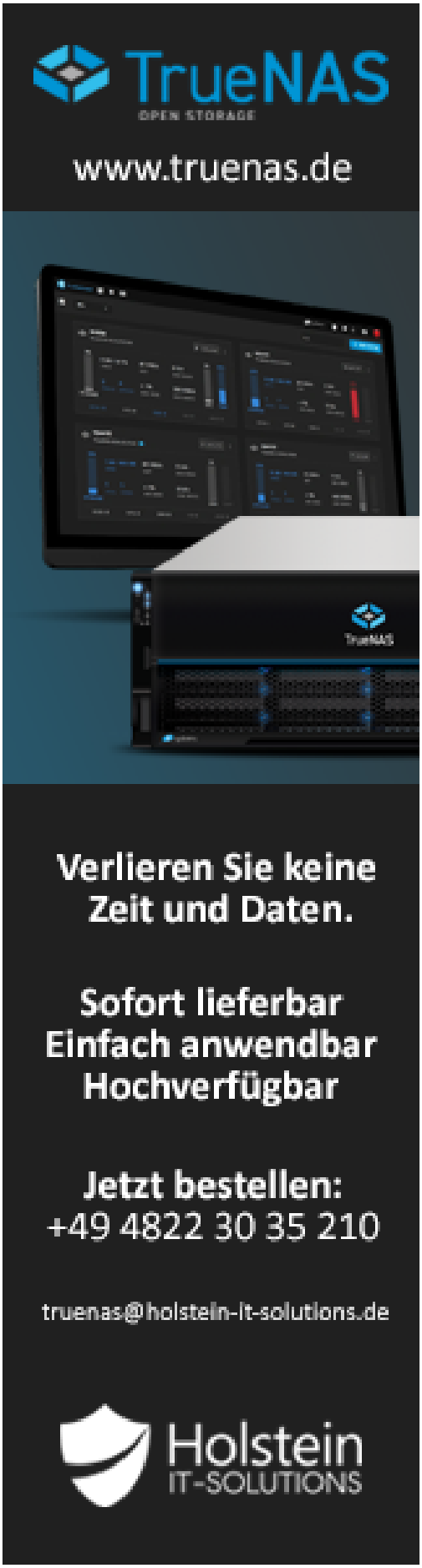
»Ein aktives, 100 Prozent sicheres Archiv kann hier helfen, wenn es zu den erzeugten Daten passt«, meint Heckel. »Tape ist keine Lösung, weil die Daten nicht verfügbar sind – und damit keiner entscheiden will/kann, welche Daten tatsächlich in dieses `tote´ Archiv verschoben werden dürfen. Die Cloud ist keine Lösung, weil die Verfügbarkeit problematisch ist, wir sind ja immer noch in Deutschland. Zudem sind die Kosten zur Nutzung schlecht vorhersagbar und potenziell sehr hoch sind. Public-Cloud-Provider können jederzeit die Preise anheben – was sie in der Vergangenheit auch gemacht haben. Wer einmal massiv Daten benötigt, beispielsweise für lokale KI-Anwendungen, wird das richtig teuer.«

Anforderungen erreichen ein neues Level

Das Datenwachstum und auch der Kostendruck ist nicht neu und begleitet den Mittelstand schon seit Jahrzehnten. Die zunehmende Wichtigkeit bzw. Abhängigkeit der Daten, die zunehmende Cyberkriminalität und auch der Fachkräftemangel, sorgen allerdings für einen neuen Level der Anforderungen.

Unternehmen stehen vor dem Dilemma, ausreichend Kapazitäten für zunehmend datenintensive Anwendungen bereitzustellen, während sie gleichzeitig mit steigenden Preisen und Beschaffungsproblemen konfrontiert sind. Angesichts dieser Herausforderungen gewinnt die Flexibilität von Storage-Lösungen an Bedeutung. Die Branche tendiert zu einer hybriden Strategie, die sowohl Cloud-Optionen als auch On-Premises-Lösungen berücksichtigt, um eine effiziente und kostengünstige Speicherverwaltung zu ermöglichen.

Auch wenn es platt klingt, angesichts dieser Entwicklungen ist es für Unternehmen ratsam, ihre Storage-Strategien zu überdenken und anzupassen. Eine ausgewogene Kombination aus moderner Technologie und strategischer Planung kann dabei helfen, sowohl den aktuellen Anforderungen gerecht zu werden als auch zukünftige Herausforderungen proaktiv anzugehen. Einfach nur auf den kleinmöglichen Nenner zu setzen, könnte sich als nachteilig erweisen. ■



Anwenderbericht mit dem IT-Dienstleister MMiT

DIGITALE INFRASTRUKTUR AUS DEM RECHENZENTRUM MIT OPEN-E JOVIANDSS

Der IT-Dienstleister MMiT benötigte eine neue (bezahlbare) Hochverfügbarkeits-Lösung, aufgeteilt in zwei Brandabschnitte. Die Storage-Systeme sollten nicht nur schnell, sondern auch skalierbar sein. Zudem standen eine lange Vorhaltezeit der Datenbestände im Pflichtenheft sowie eine kurze Wiederherstellungszeit. Die Wahl fiel auf »Open-E JovianDSS«-Systeme von N-TEC.

Sven Meyerhofer
N-TEC

Jederzeit und überall hohe Datenverfügbarkeit garantieren zu können, ist mittlerweile keine Frage des Standortes mehr. Stetige Veränderungen am Markt und individueller Handlungsbedarf sind die Grundvoraussetzungen um als Cloud- und Internet Service Provider adäquat auf die Kundenwünsche reagieren zu können.

Die in Kiel ansässige **MMiT** agiert aus dem Norden Deutschlands als regionaler und überregionaler IT-Dienstleister auf höchstem Niveau, direkt aus Deutschlands Internet-Knotenpunkt, Frankfurt am Main. Umfangreiche Service-Leistungen jeglicher Art werden hierbei direkt aus dem TÜV-zertifizierten Rechenzentrum für alle Kunden bereitgestellt.

Durch Wachstum motiviert sah sich MMiT in der Pflicht allen Kunden aufgrund gestiegener Anforderungen, die entsprechende Rechenleistung im Bedarfsfalle zur Verfügung zu stellen, und künftige Planungssicherheit zu schaffen. Zusätzlich sollte das gesuchte System in der Lage sein, Schutz vor alltäglichen Gefahren wie z.B. Ransomware zu bieten und eine schnelle Wiederherstellung der Daten zu gewährleisten.

Besondere Gewichtung lag auf dem Aspekt der Kostenkontrolle. Eine sinnvolle Investition mit einem guten Preis-Leistungs-Verhältnis stand vorrangig zur Diskussion. Im Hinblick auf die gebotenen Enterprise-Features war das ZFS-Filesystem zweifelsohne in die engere Auswahl gekommen, da es Datenintegrität und Hochverfügbarkeit kompromisslos vereinbart.

Im Zuge dessen sollten die bisher vorhandenen Geräte unter *Windows Server* bzw. *Hyper-V* abgelöst werden und die Grundlage für eine wandelbare Infrastruktur zu schaffen, samt Umstieg des Hypervisors auf **Proxmox**.

Cluster-Lösung mit intuitiven Backup

Mit all den genannten Wünschen für ein solches Cluster-System samt intuitiver Backup-Lösung wandte sich **Oliver Timm**, der Geschäftsführer von MMiT, vertrauensvoll an den Münchner Server- und Storage-Spezialisten **N-TEC**.

Infolge der langjährigen Erfahrung und positiven Ergebnisse der letzten Projekte mit N-TEC und **Open-E**, wurde ein voll-redundantes Speichersystem mit *JovianDSS* als software-seitige Lösung (SDS) vorgeschlagen.

Das Konzept sah eine zwei Knoten Konfiguration vor, welche als aktiv-aktiv Metro-Cluster eingerichtet wurde, sodass ein Lastenausgleich und deutlich erhöhte Performance erreicht wird. Der Einsatz von reinem Flash-Speicher in Form von SSDs sorgte ebenfalls für gute Synergien und harmoniert perfekt mit den restlichen Qualitätskomponenten.

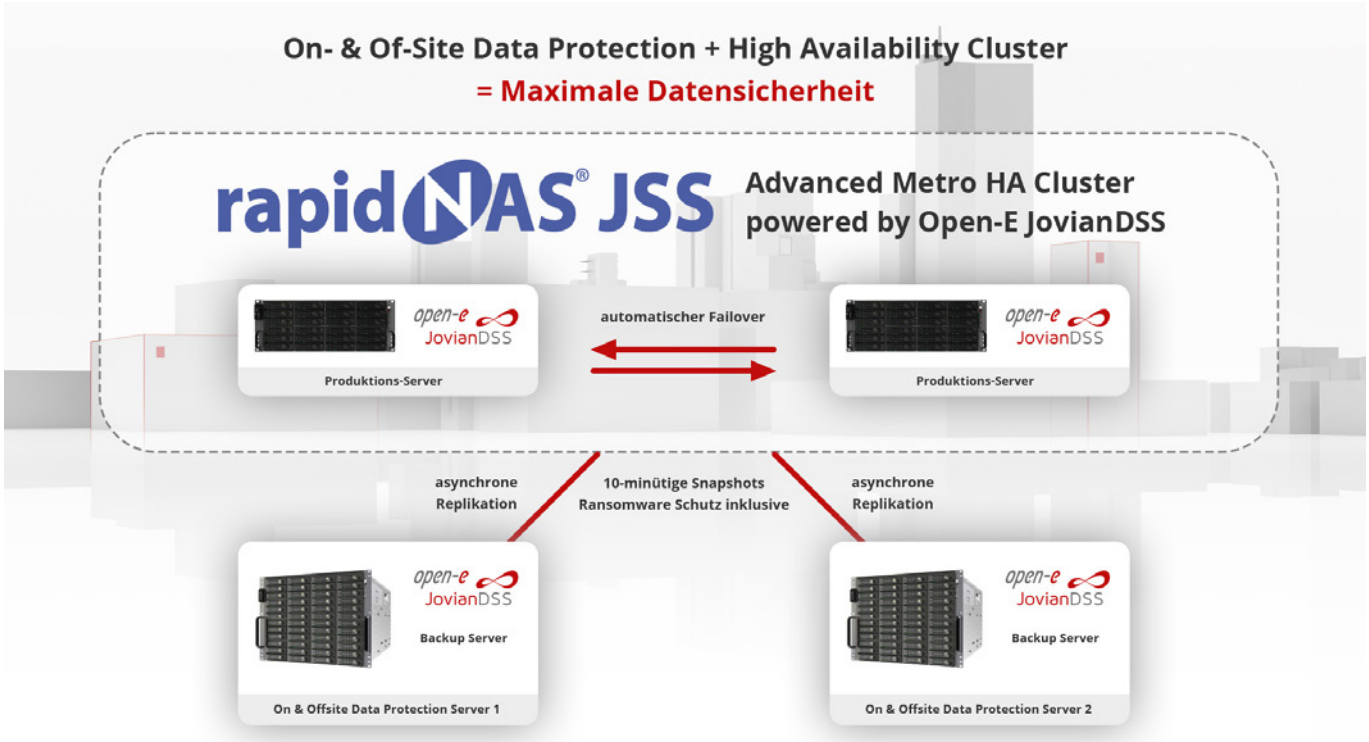
Foto: N-Tec

rapidNAS JSS224-G8 mit vier 10GbE-Ports und 15 TByte Nutzkapazität.

Die synchrone Datenspiegelung beider Server über Ethernet ermöglicht eine räumliche Distanz von bis zu zir-

Geschäftsziele & Anforderungen an die IT:

- Bezahlbare Hochverfügbarkeit, zwei Brandabschnitt-Lösung im Rechenzentrum lange Vorhaltezeit der Datenbestände im Backup-Server (Snapshots)
- Schnelle und flexible Storage-Erweiterungsmöglichkeiten
- Kurze Wiederherstellungszeit hohe Datenintegrität



Grafik: N-Tec

Bildliche Darstellung des Konzeptes samt Metro-Cluster und On & Offsite Data Protection (OODP)

ka 50 Kilometer und konnte somit im Rechenzentrum selbst, ebenso in verschiedenen Zonen aufgeteilt werden, sodass zusätzliche Sicherheit geschaffen wird.

Besonderes Augenmerk lag jedoch auf dem dritten Knoten in dieser Konstellation. Mit *On & Offsite Data Protection* von Open-E JovianDSS ist dieser extra Server in der Lage – direkt vom Metro-Cluster – voll konsistente Snapshots im Minutentakt zu erhalten und abzuspeichern. Diese ZFS-Technologie erlaubt den Aufbau extrem vielseitiger Backup-Lösungen und Strategien. MMiT ist somit in der Position, die gewünschten Datenbestände der Vergangenheit, granular aufzugliedern, und zu beliebigen Zeitpunkten zurückzukehren, welche vorher definiert wurden. Mit dem Einsatz von zum Beispiel Windows kann bequem per rechten Mausklick auf den Dateistand geblickt werden, und auf vorherige Versionen zurückgegriffen werden.

Die Cleverness dieser Lösung besteht darin, dass lediglich die sogenannten »Delta-Daten« sprich Daten, welche sich währendes des Arbeitsalltags bzw. innerhalb der Snapshot-Zyklen geändert haben, repliziert werden.

Somit entsteht, je nach zeitlich definiertem Intervall, eine regelmäßige Übertragung bzw. regelmäßiges Backup. Dank dieser eleganten Lösung wird ein vollständiges Backup alle zehn Minuten herbeigeführt, und reduziert die Belastung des Netzwerkes auf ein Mindestmaß. Die tägliche administrative Routine-Arbeit eines mühsamen Backups während der Mittagszeit oder nach Feierabend entfällt somit gänzlich.

Administration spürbar schneller und einfacher

»Zusammenfassend bin ich begeistert von der Open-E-Software JovianDSS«, sagt MMiT-Geschäftsführer Timm. »Unzählige administrative Möglichkeiten samt voll automatisieren Backups Rund-um-die-Uhr haben unseren Alltag spürbar erleichtert. N-TECs Herangehensweise an dieses Projekt war außerordentlich angenehm und überzeugend. Alle Erwartungen wurden letztlich – vollends erfüllt - und in den meisten Fällen gar weit übertroffen. Nicht nur unsere Kunden profitieren enorm von dieser Professionalisierung, sondern auch wir selbst, da wir unseren zeitlichen Aufwand in vielen Tätigkeitsbereichen drastisch reduzieren konnten.

Gerade die Option, Datenzustände – jederzeit, in kürzester Zeit – wiederherstellen zu können, gibt uns ein Gefühl von Sicherheit. Unsere Kunden können darauf vertrauen, dass Bedrohungen wie Ransomware-Angriffe ein Phänomen bleiben, welches wir lediglich von den Medienberichten kennen.

Ich freue mich schon auf die Erweiterung unseres Haupt-Systems und die Anschaffung des zweiten Backup-Servers. Durch den kontinuierlichen Wachstum konnten wir all unsere Systeme mit Festplatten und Lizenzen aufstocken und bedarfsgemäß im wirtschaftlichen Sinne reagieren.« ■

Weitere Informationen:

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

ANZEIGE

Das aktive WORM-Archiv

ARCHIVIERUNG ALS TEIL MODERNER DATENSICHERUNG

Hannes Heckel
FAST LTA

Ein Archiv galt lange Zeit als »Datenfriedhof«, als letzte Instanz für Daten, auf die man (hoffentlich) nie wieder zugreifen muss. Doch ein aktives WORM-Archiv kann helfen, die Datensicherung zu verschlanken, Kosten zu sparen und sich für zukünftige Anforderungen zu rüsten.

In vielen Filmen werden Beamte nach Fehlern zur Strafe ins Archiv versetzt. Dunkle Räume mit Gängen voller Akten, die außer dem Archivar fast nie jemand zu Gesicht bekommt. Oft retten aber das Archiv und der allwissende Archivar am Ende den Helden, weil nur dort noch Informationen zu finden sind, die entscheidend für den Ausgang der Handlung sind.

Dieses Bild vom Archiv hat es bei vielen auch ins digitale Zeitalter geschafft: Daten, die im Archiv landen, sind schwer zugänglich und nur mit viel Aufwand überhaupt nutzbar. Das Archiv ist der Friedhof für Daten, die man (hoffentlich) nie wieder benötigt. Solche Daten können in so genannten »kalten Archiven« verschwinden – oder, wenn keine rechtlichen Gründe entgegenstehen, eigentlich auch gelöscht werden.

Die Kernfrage: Welche Daten?

Damit stellt sich aber eine entscheidende Frage: Wer entscheidet, welche Daten ins Archiv verlagert werden? Eigentlich der Erzeuger der Daten, also der Anwender. In der Praxis ist das nicht realistisch, da sich Anwender selten um Datenmanagement kümmern. So bleibt diese Aufgabe am IT-Verantwortlichen hängen. Der kann aber oft nicht einschätzen, welche Daten tatsächlich »nicht mehr benötigt« werden und ins Archiv wandern. Im Zweifel entscheidet man, viel mehr Daten in Produktivumgebungen zu belassen, als eigentlich notwendig wäre. Die Folge: Kosten für Produktiv-Storage und Datensicherung steigen ständig an. Im Zeitalter von Ransomware, wo unterschiedliche Backup-Bereiche dann noch per Immutability besonders abgesichert werden müssen, erhöht dies zusätzlich die Komplexität der Datensicherung.

Das aktive Archiv

Archivspeicher, die nicht auf reinen Offline-Medien (wie Tape) basieren, lassen sich hingegen als »aktives Archiv« betreiben. Die Idee: Auch wenn Daten von den Produktivsystemen ins aktive Archiv verdrängt werden, bleiben sie jederzeit verfügbar. Es geht also darum, Daten zu identifizieren, die nicht mehr verändert werden (dürfen), so wie in zunehmendem Maße automatisch erzeugte Daten. Die frühzeitige Auslagerung dieser Daten verschlankt die Datensicherung erheblich, spart Kosten und reduziert die Komplexität.

Das aktive WORM-Archiv

Cyber-Angreifer nehmen fast immer zuerst die Datensicherung ins Visier, um eine zuverlässige Wiederherstellung manipulierter Daten zu verhindern. Aktive Archive brauchen somit besonderen Schutz. Höchste Sicherheit bieten Speichersysteme mit unüberwindbarer Hardware-Versiegelung: WORM-Speicher.

Das moderne Archiv

Ein modernes Archiv ist als zentrale Komponente der Datensicherung zu sehen, um regelmäßige Backups zu reduzieren und die Komplexität für Backup und Recovery ganz allgemein zu minimieren. Wahlfreier, schneller Zugriff gewährleistet die Verfügbarkeit ausgelagerter Daten, eine Versiegelung per Hardware-WORM garantiert maximalen Schutz.

Damit werden der Archivierung mehrere Hürden genommen.

1. Es ist relativ klar, welche Daten ins (aktive) Archiv ausgelagert werden können: auf jeden Fall alle automatisch erzeugten, nicht reproduzierbaren Daten. Vorsicht ist bei personenbezogenen und anderen sensiblen Daten geboten, die zumeist besondere, revisionssichere Archivsysteme erfordern.
2. Es spielt keine Rolle, wenn »zu viele« Daten im Archiv landen. Im schlimmsten Fall wird bei Veränderung eine neue Version des Datensatzes angelegt. Je mehr Daten ins aktive Archiv verschoben werden, desto schlanker wird die Datensicherung.
3. Denn: Die Daten sind nach wie vor verfügbar. In vielen Fällen sorgt eine Archiv-Software für Datentranspar-

Foto: FAST LTA

Die neuen Silent Cubes DS (Pro) lösen die bewährten Silent Cubes im Würfel-Design (hinten) ab.

enz, dann merken Anwender noch nicht einmal, wo die Daten letztlich gespeichert werden. Oder das aktive Archiv agiert wie ein Netzwerkspeicher (NAS), auf den Anwender mit üblichen Mitteln zugreifen können.

4. Die WORM-Versiegelung schützt die Daten von Anfang an hundertprozentig vor Manipulation und ungewolltem Löschen. Eine Datenmanipulation würde in einem WORM-Archiv nur neue Versionen erzeugen, die hierbei benötigte Kapazität plötzlich stark ansteigen. So lassen sich solche Angriffe relativ leicht erkennen. Zum Schutz vor menschlichem Versagen und Technik-Ausfällen muss der Archivspeicher zudem über genügend lokale und Geo-Redundanz verfügen.

Technologien: Tape, Cloud, Disk/Flash

Tape gilt als klassisches Archivmedium und bietet für »kalte Archive« auch konkrete Vorteile. Die Medien sind günstig, lassen sich sicher offline lagern, und die Kapazität lässt sich im Grunde unbegrenzt erweitern. Daten auf Tapes sind aber eben »kalt« und erst nach Zurückspielen auf ein anderes Speichersystem wieder verwendbar. Ein aktives Archiv lässt sich so nicht realisieren.

Immer populärer wird die Auslagerung von Daten in ein Cloud-Archiv. Dies kann für kleine Unternehmen sinnvoll sein, weil keine Investition in spezielle Speichersysteme notwendig ist. Auch die Kosten erscheinen zunächst niedrig. Oft kosten Einlagern (Hochladen) und Aufbewahrung nichts oder sehr wenig. Kosten entstehen hingegen beim Datenabruf. Dabei gibt es oft mehrere Stufen, je nach gewünschter Verfügbarkeit. Für seltenes bzw. einmaliges Abrufen mag das akzeptabel sein, jedoch hat die Vergangenheit gezeigt, dass Anbieter ihre Preise nach Belieben erhöhen können – und dies auch tun. Spätestens, wenn Daten immer wieder und in großen Mengen für lokale Auswertungen (KI) benötigt werden, stellt sich die Frage nach der Wirtschaftlichkeit. Problematisch kann die mangelnde Transparenz über die tatsächliche Speicherung sein, insbesondere, wenn es um Daten geht, die der DSGVO unterliegen.

So bleiben lokale bzw. private Speichersysteme, die auf nicht-linearen Medien wie Festplatten oder Flash basieren. Standard-Storage erfüllt allerdings in den meisten Fällen nicht die Voraussetzungen, um als ein aktives WORM-Archiv eingesetzt zu werden, das auch preislich mit den genannten »Alternativen« mithält. Aktive WORM-Archive auf Festplatten- (oder Flash-) Basis sind deshalb speziell für diesen Zweck entwickelte Speichersysteme.

Silent Cubes

Seit über 15 Jahren sichern *Silent Cubes* Archivdaten mit genau diesen Merkmalen. Ursprünglich für die revisionssichere Archivierung zur Einhaltung rechtlicher Vorgaben entwickelt, werden Silent Cubes zunehmend als generelle, aktive WORM-Archive eingesetzt. Neben WORM-Versiegelung per Hardware verfügen sie über weitere Technologien zum Schutz vor Manipulation und Datenverlust. Innerhalb eines Speichermoduls werden Daten per Erasure-Coding mit vierfacher Redundanz vor Hardware-Ausfall geschützt. Geo-Redundanz bewahrt vor dem Ausfall kompletter Systeme. Da das System modular aufgebaut ist, können einzelne Speichermodule bei Nichtbenutzung in Standby mit extrem niedrigem Energieverbrauch geschaltet werden. Umfangreiche, flexible Wartungsvereinbarungen sorgen zudem für zehn und mehr Jahre reibungslosen Betrieb. ■

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

ANZEIGE

actidata Q-DX6: Integriertes Festplatten-Wechselsystem von 4 bis 40 TByte

DATENSICHERUNG FÜR KLEINERE IT-UMGEBUNGEN

Speziell an IT-Umgebungen der Einstiegsklasse richtet sich der Backup-Server actidata Q-DX6. Der NAS-Speicher bietet eine Kapazität von bis zu 40 TByte und ist zudem mit einem integrierten Wechselplattensystem ausgestattet. Damit lassen sich Sicherungen auch auslagern.

Albrecht Hestermann
actidata

Mit dem *Q-DX6* Backup-Server stellt **actidata** ein kompaktes Windows-Server basierendes System vor, bei dem ein bewährtes 3,5-Zoll-Wechselplattensystem von der *CRU Data Security Group* eingebaut ist. Als Disk-basierender NAS-Datenspeicher sind vier 24x7 Enterprise Festplatten im Quasi-RAID10 (Storage Spaces) eingebaut, das mit einer optionalen *HotSpare*-Festplatte aufgerüstet werden kann. Installiert in einem anderen Brandabschnitt stellt der actidata Q-DX6 Backup-Server bis zu 40 TByte Nettokapazität als NAS-System über die eingebaute 10-Gbit-Ethernet-Schnittstelle zur Verfügung. Die nötige, zusätzliche Datensicherung auf die auswechselbaren DX6-Medien zur Auslagerung der Backup-Sätze erfolgt intern mit einer Datentransferrate von bis zu 250 MByte/s.

Bild: actidata

actidata DX6: NAS-Speicher in Desktop-Bauform mit integriertem DX6-Wechselfestplattensystem.

Konsequent auf 24x7 Server-Komponenten gesetzt

Server-Komponenten, die im actidata Q-DX6 eingesetzt werden, sorgen für eine hohe 24x7-Betriebssicherheit und optimale Performance sowohl zu den Produktivsystemen über die eingebaute 10-Gbit-Ethernet-Schnittstelle als auch intern auf die bis zu 900 MByte/h schnellen Festplatte im DX6-Wechselmedium. Die Verwaltung und Überwachung der Hardware erfolgen über eine separate IPMI-Board-Management-Schnittstelle. Für das Betriebssystem und das Disk-System wird hierzu eine SNMP-Überwachung bzw. die integrierte Überwachungsapplikation benutzt.

actidata DX6 – Das actidata Medien-Auswechselsystem

Als Datenträgerbasis setzt actidata auf ein Wechselplattensystem der *CRU Data Security Group*. Ausgestattet mit für den 24x7-Betrieb ausgelegten Enterprise-SATA-Festplatten im 3,5-Zoll-Format und kombiniert mit einem 3-jährigen Vorabaustausch-Service vereint actidata in den DX6-Medien Komponenten und Services mit Leistungsmerkmalen, die seitens der Anwender gefordert werden. Als actidata DX6-Medium stehen aktuell Kapazitäten von 4, 8, 12 und 20 TByte zur Verfügung. Weitere Kapazitätsklassen werden inline mit den Weiterentwicklungen der 3,5-Zoll-Festplatten-Klasse folgen.

Konzipiert als offenes System

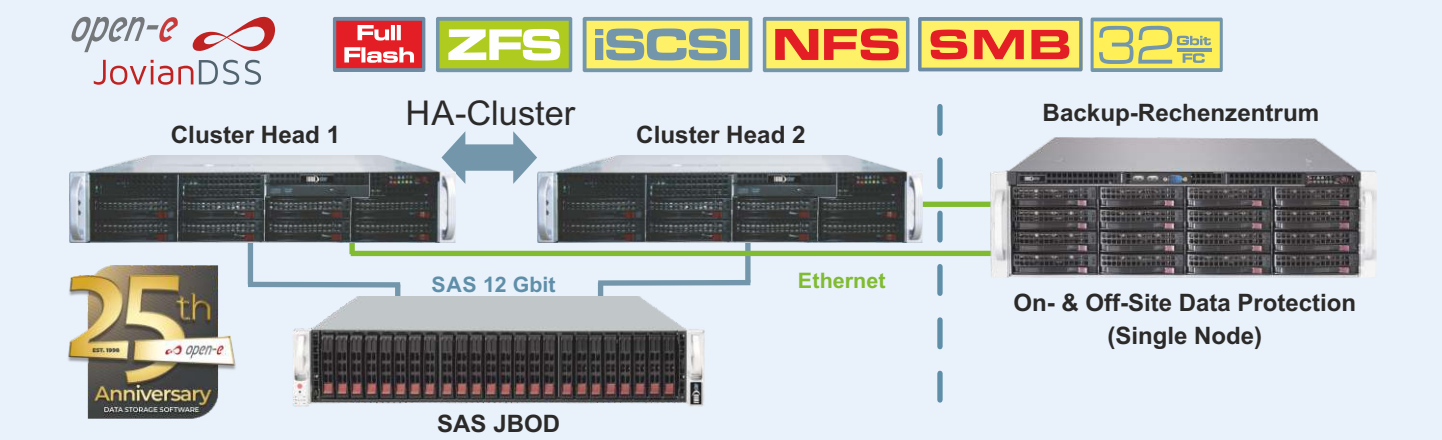
Der Windows-Server-basierende actidata Q-DX6 Backup-Server eignet sich besonders für den Einsatz als Datensicherungssystem in IT-Systemumgebungen der Einstiegsklasse. Im Rahmen eines »Backup-to-Disk-to-DX6«-Datensicherungskonzeptes steht für das Disk-basierende Backup dank Windows Server 2022 der Speicherplatz über SMB-Freigaben bereit. Auch das anschließende Backup auf das auswechselbare actidata DX6-Medium erfolgt durch eine handelsübliche Backup-Software. Ohne Zusatzkosten liegt dem actidata Q-DX6 die SW-Lösung von *IPERIUS* bei, jedoch kann auch in eigener Regie eine andere, Windows-Server kompatible Backup-Software, die Wechseldatenträger unterstützt, eingesetzt werden. ■

Weitere Informationen:

actidata Storage Systems GmbH
Wulfshofstr. 16 – Indu-Park,
44149 Dortmund
Tel: 0049 (0) 231/96 36 32 – 0
E-Mail: info@actidata.com
www.actidata.com

Open-E JovianDSS ZFS Cluster mit neuen Features

Storage Cluster mit **Open-E JovianDSS** sichern die Verfügbarkeit der Daten sowohl durch die Active/Active Redundanz der Clusterknoten als auch durch die Fehlertoleranz des **ZFS** Filesystems. Mit dem neuen Release, das derzeit in Vorbereitung ist, werden außer dem ZIL- und Readcache auch sogenannte **„ZFS Special Devices“** unterstützt. Das ist ein SSD Schreibcache für Metadaten und kleinere Datenpakete, wodurch eine Performancesteigerung erzielt wird. Auch bei der snapshotbasierten Sicherung der Daten in ein ODP System (**On- & Off-Site Data Protection**) bringt die neue Version Vorteile: Komprimierte Daten werden zur Synchronisation nicht mehr entpackt, sondern direkt als „raw data“ übermittelt, was vor allem bei geringer Netzwerk-Bandbreite den Durchsatz verbessert.



ES-8700JDSS Cluster mit iSCSI/NAS zu den Clients + ODP Schutz vor Ransomware

zwei Cluster Knoten, active/active, je 4 x 10 GbE Hostanbindung + 24-Slot Shared Storage SAS JBOD, teilbestückt: 12 x 3,84 TB SAS SSD (2 vdevs RAID-Z2, 25,2 TiB), inkl. Open-E JovianDSS Lizenzen, Preis zzgl. Installation

inkl. MwSt. **€ 32.011,-** exkl. MwSt. **€ 26.900,-**

16-Slot Server System, On- & Off-Site Data Protection System für den Cluster, teilbestückt mit 9 x 12 TB Nearline SAS Disks (1 vdev RAID-Z3, 59 TiB usable), inkl. Open-E JovianDSS Lizenzen

inkl. MwSt. **€ 13.673,10** exkl. MwSt. **€ 11.490,-**

ES-8700JDSS Cluster und Backup System

- 2 HE Cluster Knoten mit zwei Intel Xeon 4215R Prozessoren, 8 Core, 3.2 GHz auf X11 Board, 192 GB RAM,
- 2 x 10 GbE RJ45 (opt. SFP+) für Interconnect + 2 x 10 GbE (SFP+) zu den Clients (optional bis 100 GbE und FC Ports)
- JBOD: 12 Gbit SAS 24, 2 HE (opt. mehrere JBODs)
- On- & Off-Site Data Protection: 3 HE 16-Slot Server Intel Xeon 6134 Prozessor, 8 Core, 3.2 GHz auf X11 Board, 128 GB RAM, 2 x 10 GbE RJ45, opt. weitere Ports bis 100 GbE
- IPMI 2.0 RJ45 Port für Überwachung / Remote Management
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

Als zusätzlicher Schutz lassen sich die SSDs zweier JBODs untereinander spiegeln. Mit 3 JBODs können auch RAID-Z2 vdevs aus je 2 SSDs pro Box realisiert werden.

Open-E JovianDSS iSCSI/NAS/FC Software:

- ZFS 2.0 Filesystem für maximale Datenintegrität
- Schutz vor „Stealth Errors“ durch Check-Summen-Prüfung und Disk-Scrubbing
- Plattenredundanz durch Mirror, RAID-Z, -Z2, -Z3 (entspricht RAID 1, 5, 6 und dreifacher Parity)
- SSDs zur I/O-Beschleunigung (Read/Write-Cache)
- konfigurierbar als shared Storage active/active Cluster
- praktisch unbegrenzte Snapshots und mountbare Snapshot-Volume-Clones ohne Performanceverlust
- iSCSI, NFS und CIFS/SMB Volumes, opt. Fibre Channel
- Thin- und Thick-Provisioning
- LZ4 Datenkompression und inline Deduplikation
- On- & Off-Site Data Protection zur Datensicherung auf weiteres System, Reaktivierung in wenigen Minuten
- intuitive Web-GUI für einfaches Management
- 3 Jahre Open-E Standard Support (E-Mail und Telefon), optional erweiterte Open-E Services
- Installation und Konfiguration vor Ort / remote durch EUROstor (berechnet nach Aufwand)

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, Scale-Out Clustern, Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die Server-Virtualisierung. Registrieren Sie sich einfach unter www.EUROstor.com/Newsletter, oder rufen Sie uns an!

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

Preisänderung, Druckfehler und Irrtum vorbehalten.

ANZEIGE

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 Franz Bochtler. Für die technische Leitung verantwortlich ist Wolfgang Bauer. 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.

N-TEC GmbH

n-tec.eu

Sitz der Gesellschaft:
Ismaning

Jahr der Gründung:
2001

Zielgruppe:
Vor allem KMU + öffentliche Auftraggeber

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

Quantum

quantum.com/de

Sitz der Gesellschaft:
San Jose, USA

Niederlassungen in Deutschland:
München

Jahr der Gründung:
1980

Zielgruppe:
Mittelständische und große Unternehmen

Mit Technologien und Services von Quantum lassen sich digitale Inhalte erfassen, verarbeiten und gemeinsam nutzen – und außerdem für Jahrzehnte vorhalten und sichern. Unsere Plattformen bieten die schnellste Performance für große Datenmengen, industrielles IoT und hochauflösendes Film- und Bildmaterial – für jede Phase des Datenlebenszyklus – von der Kollaboration und Analyse in Echtzeit bis zur kostengünstigen Archivierung.

tproneth

tproneth.de

Sitz der Gesellschaft:
Pucheim

Jahr der Gründung:
1999

Zielgruppe:
mittelständische Industrieunternehmen, Behörden, Bildungseinrichtungen, Gesundheitswesen

tproneth ist ein IT-Dienstleistungsunternehmen in München, das überregional Kunden ganzheitlich in Sachen IT berät, IT-Lösungen erarbeitet und sie bei Implementierung und Betrieb unterstützt. Unsere Mission: Realisierung leistungsstarker Rechenzentren, die für unsere Kunden nicht nur erschwinglich sind, sondern auch technologisch und wirtschaftlich sinnvoll. Neu: Wir haben im Partnerprogramm Sphere von NetApp das hohe Prestige-Level erreicht. Seit über 10 Jahren gehen wir bereits gemeinsame Wege. Dank seines nachhaltigen Wachstums und seines tiefen technischen Know-hows wurde uns der Prestige-Partnerstatus verliehen.

Holstein IT-Solutions

truenas.de/

Sitz der Gesellschaft:
Hagen

Jahr der Gründung:
2015

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

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

Actidata

actidata.com

Sitz der Gesellschaft:
Dortmund

Niederlassungen in Deutschland:
Dortmund

Jahr der Gründung:
2009

Zielgruppe:
Systemhäuser, VARs und Industriekunden

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

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.

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.

Cyberabwehr 2023: KMUs im Fokus von Ransomware

DATEN IN GEFAHR: CYBERKRIMINELLE IMMER PROFESSIONELLER

Karl Fröhlich
speicherguide.de

Der Mittelstand sieht sich mit einer wöchentlichen Flut an Cyberangriffen konfrontiert und kämpft tagtäglich gegen 250.000 neue Malware-Varianten an. Um die Cyberresilienz zu stärken, rücken deshalb Strategien zur Abwehr von KI-gestützten Ransomware-Angriffen in den Fokus. Sicherungen müssen geprüft und unveränderlich sein.

Bei aller Storage-Technik, Thema Nummer eins bleibt die Abwehr von Cyberangriffen und wie sich IT-Abteilungen bestmöglich dagegen schützen können. Ransomware sorgt definitiv für Verunsicherung. Nach bisherigen Erkenntnissen wird eine Organisation im globalen Schnitt wöchentlich 1.200 mal angegriffen. In Deutschland waren in den ersten drei Quartalen 2023 wöchentlich 386 Organisationen von einem Cyberangriff betroffen.

Der wirtschaftliche Schaden von Ransomware ist erheblich, insbesondere für kleine und mittlere Unternehmen sowie kommunale Einrichtungen. Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) registriert 2023 täglich etwa 250.000 neue Varianten von Malware und 21.000 infizierte Systeme. Darüber hinaus wurden durchschnittlich 70 neue Sicherheitslücken pro Tag entdeckt, von denen die Hälfte als hoch oder kritisch eingestuft wurde – ein Anstieg um 24 Prozent im Vergleich zum Vorjahr.

Die anhaltende Digitalisierung und zunehmende Vernetzung vergrößern die Angriffsflächen – und diese werden genutzt. »Wir verzeichnen einen Anstieg der Bedrohung im Bereich Schwachstellen«, sagt BSI-Präsidentin **Claudia Plattner.** »So werden täglich knapp 70 neue Schwachstellen in Software-Produkten entdeckt – rund 25 Prozent mehr als im vorherigen Berichtszeitraum. Auch die rasante Weiterentwicklung neuer und angepasster Angriffsmethoden und der zunehmende Dienstleistungscharakter (Cybercrime-as-a-Service) sind besorgniserregend.«

Cyberkriminelle immer professioneller

Erschwerende Tendenz: Während KMUs, gefühlt auf der Stelle treten, werden Angreifer im Cyberraum zunehmend professioneller. Sie nutzen vermehrt arbeitsteilige Prozesse und künstliche Intelligenz (KI), um gezielte

Grafik: Dall-E (KI)

Angriffe durchzuführen. Vor allem der zunehmende Einsatz von KI ist besorgniserregend. Mit gefälschten Bildern und Videos wird einerseits Desinformation und Cybermobbing betrieben, gleichzeitig ist auch die Zeit schlecht übersetzter Spam-Mails vorbei. Auch die Gefahr von Cyberspionage nimmt zu, die oft politisch motiviert ist und auf Einflussnahme abzielt.

»Die logische Konsequenz aus alldem – nicht neu, aber laut **Hannes Heckel**, Leitung Marketing bei **FAST LTA,** entscheidend: »Digitale Strukturen müssen geschützt werden und die Verbreitung von Falschinformationen muss eingedämmt werden. Oberste Priorität sei es dafür, dass Politik, Wirtschaft und Wissenschaft eng zusammenarbeiten - in den Kommunen, den Ländern und im Bund, in Europa sowie international.«

»Unsere oberste Priorität ist es, Deutschland digital und sicher aufzustellen«, ergänzt BSI-Präsidentin Plattner. »Das gelingt nur mit koordinierter Zusammenarbeit aller Akteure in den Kommunen, den Ländern und im Bund, international sowie in ganz Europa. Dabei gilt es, auch in den Austausch mit Wirtschaft, Wissenschaft und Gesellschaft zu treten. Wir verstehen Cybersicherheit als Gemeinschaftsaufgabe, die auf Transparenz als Grundlage für Vertrauen beruht.«

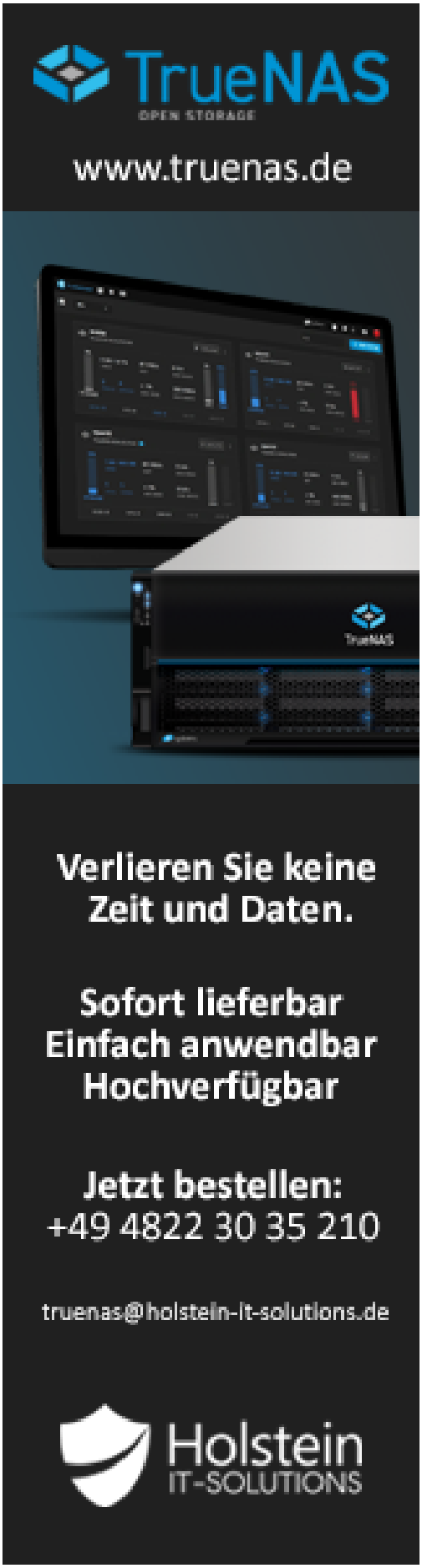
Bei aller Verunsicherung im Mittelstand, es gibt auch Grund zur Hoffnung: »Viele Unternehmen beginnen inzwischen zu verstehen, dass vor allem Backup-Dateien Ziele von Hackerangriffen sind und auch der Mittelstand davon betroffen ist«, erklärt **Patricia Hillebrand**, International Channel Manager bei **RNT Rausch.** »Nur weil Datenvolumen im Mittelstand kleiner sind, sind diese Daten nicht weniger wertvoll und müssen daher ebenso gut geschützt werden wie die großen Datenmengen im Konzernumfeld.«

Kontrollierte Datenwiederherstellung

»Das FBI stellt gerade den Trend zu so genannten »dualen Ransomware-Angriffen« fest«, erklärt **Mark Molyneux,** EMEA CTO bei **Cohesity**. »Cyberkriminelle führen hierbei zwei oder mehr Attacken in kurzer Folge durch. CIOs und CISOs suchen nach Wegen, um aus einer solchen Endlosschleife aus Angriff, Wiederherstellen und erneutem Angriff mit höherem Risiko auszubrechen. Wichtig ist dabei, den gleichen Fehler nicht zwei mal zu machen. In der Krise während einer Cyberattacke arbeiten Mitarbeiter der IT-Teams unter Hochdruck und Stress daran, den Karren aus dem Dreck zu ziehen. Wichtige Systeme sollen schnell wieder laufen, Kunden und Partner richtig informiert werden. In dieser Extremlage kommt es zu einem verhängnisvollen Fehler. Die Systeme werden aus bestehenden Backups rekonstruiert, damit sie schnell wieder laufen. Es ist verführerisch, möglichst frische Kopien zu nehmen, da dies den möglichen Datenverlust klein hält. Die Systeme werden in einen jungen Zustand wiederhergestellt – und damit leider auch alle feindlichen Fake-Accounts, kompromittierten Passwörter, ungepatchte Schwachstellen in den Be-

»Wir entdecken täglich knapp 70 neue Schwachstellen in Software-Produkten.«

Claudia Plattner, BSI



triebssystemen, Artefakte bereits eingeschleuster Schadcodes.«

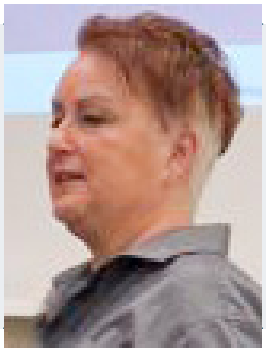
Molyneux empfiehlt eine Art Reinraum, als sinnvolle Alternative für dieses Vorgehen. In einer isolierten Umgebung können alle beteiligten IT-Teams parallel mit Kopien der Produktionsdaten arbeiten. Mithilfe von Datenmanagement-Lösungen stehen Snapshots von unterschiedlichen Systemen in bis zu 90 Tagen alten Versionen entlang der verschiedenen Phasen der Vorfallzeitleiste zur Verfügung.

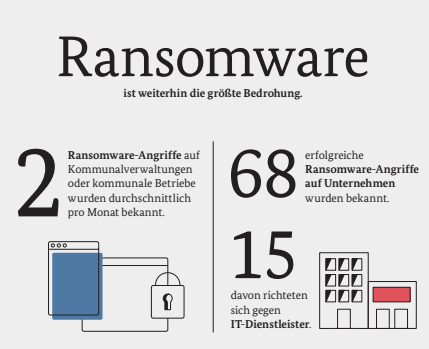
»Moderne Datensicherheits- und Verwaltungsplattformen können diese Snapshots in einer isolierten Umgebung bereitstellen, die dank Vaulting, Immutable-Storage, Multi-Faktor-Authentifizierung und Verschlüsselung gegen externe Angriffe geschützt sind«, meint Molyneux. »Auf Systemen, die unverschlüsselt blieben, haben Angreifer häufig so genannte Persistenz-Mechanismen versteckt. Daher sollten IT-Sicherheitsteams im gesamten Bestand nach Kompromittierungs-Indikatoren suchen und dabei die schnellen Indizierungs- und Suchfunktionen der Datenverwaltung nutzen, ohne die Systeme überhaupt aufblähen zu müssen.« Die gefundenen Schwachstellen müssen gepatcht, die bösartigen Konten entfernt, die Schutz- und Erkennungskontrollen verstärkt werden, damit der gleiche Vorfall nicht erneut eintritt. Gleichzeitig müssen IT-Manager alle bösartigen Artefakte entfernen, bevor ein System in die Produktion zurückgespielt wird.

Für Molyneux ist es unerlässlich, dass sich CIO und CISO im Unternehmen untereinander abstimmen und die Prozesse zusammen justieren. Die Wiederherstellung dauert so zwar womöglich etwas länger, die Vorteile wiegen dies allerdings wieder auf: Das Risiko einer Folgeattacke sinkt und die Cyberresilienz der ganzen Umgebung steigt.

»Unternehmen beginnen inzwischen zu verstehen, dass vor allem Backup-Dateien Ziele von Hackerangriffen sind.«

Patricia Hillebrand, RNT Rausch





Wichtig ist, dass sich IT-Manager und Geschäftsleitungen frühzeitig vorbereiten. »Zu beachten ist beispielsweise, dass im Falle eines Angriffs in der Regel als erste Maßnahme alle externen Verbindungen zu kappen sind«, sagt Hillebrand von RNT Rausch. »Und zu erkennen, dass je nach verfügbarer Bandbreite die Wiederherstellung sehr lange dauert und ein einfaches NAS nicht als letzte Verteidigungslinie ausreicht.« Auch gelte es Cloud-only Backups zu überdenken. Diese seien zwar relativ günstig in finanzieller Hinsicht, aber oftmals sehr problematisch und teuer sowie langwierig im Wiederherstellungsfall. Viele Cloud-Anbieter stellen ihren Kunden nicht den Speicherplatz in Rechnung, sondern den Zugriff auf ihre Daten, sodass oft hohe und nicht eingeplante Rechnungen im Wiederherstellungsfall auflaufen.

Als sinnvolle Verteidigung gegen die Folgen eines Ransomware-Angriffs empfiehlt sich eine unveränderbare Backup-Kopie vor Ort, eine weitere Kopie auf einem anderen Medium sowie eine ausgelagerte Datenkopie an einem anderen Standort. Aufgrund der neuen Bedrohungslage sollte diese 3-2-1-Backup-Regel mit einem zusätzlichen Air-Gapped- oder Offline-Backup sowie einem Prüfprozess ergänzt werden. Man spricht hier dann von der 3-2-1-1-0 Regel.

Das Backup auf seine Richtigkeit zu prüfen, sollten IT-Manager nicht vernachlässigen, denn nur allzu oft funktionieren die Sicherungskopien nicht wie geplant. Zudem gilt auch für die Datenwiederherstellung: üben, üben, üben. ■

»Wiederherzustellende Daten sollten zuerst in einer isolierten Umgebung getestet werden.«

Mark Molyneux, Cohesity

Weitere Informationen:

- BSI: Die Lage der IT-Sicherheit in Deutschland 2023 »
- Cyberangriffe: Wöchentlich 386 Firmen in Deutschland betroffen »
- Zunahme von Cyberangriffen auf den Bildungssektor »

Wie widerstandsfähig ist Ihr Unternehmen?

2021 wurde jedes dritte deutsche Unternehmen Opfer eines Ransomware-Angriffes.

Die Kosten für die Wiederaufnahme der Geschäftstätigkeit betrugen im Durchschnitt 1,6 Mio. Euro.

Nach einem Ransomware-Angriff betrug die Zeit für ein Unternehmen bis zur Wiederaufnahme des Geschäftsbetriebes im Durchschnitt einen Monat.

Mehr als 35% der betroffenen Unternehmen können ihre Daten nach einem Angriff nicht wiederherstellen.

Ursachen für eine fehlgeschlagene Wiederherstellung von Daten

- Das Backup ist veraltet.
- Daten wurden unvollständig gesichert.
- Die Daten im Backup wurden kompromittiert.
- Die Datensicherung ist fehlgeschlagen.

Wann haben Sie Ihr Backup das letzte Mal getestet?

Scan me

Wie schnell sind Sie wieder einsatzfähig nach einem Ausfall?
Testen Sie jetzt mit uns Ihr Backup.

1) Quelle: Sophos State of Ransomware Report 2022

Die 3 häufigsten Ursachen für Ausfälle

Hardware-Ausfälle

Anwenderfehler

Korruption & Viren

TrueNAS
OPEN STORAGE

www.truenas.de

Holstein
IT-SOLUTIONS

Holstein IT-Solutions
Dorfstraße 18a
24576 Hagen

Telefon: 04822 30 35 210
E-Mail: info@holstein-it-solutions.de
Web: holstein-it-solutions.de

Vor- und Nachteile sind im Einzelfall abzuwägen

IT-MANAGER BLEIBEN BEI DER CLOUD SKEPTISCH

Karl Fröhlich
speicherguide.de

Skalierbarkeit, automatisierte Updates und Wartung und eine Zusammenarbeit in Echtzeit sprechen für Cloud-Strukturen. Gleichzeitig besteht eine Abhängigkeit von Internetverbindungen und von eigenen Sicherheitsmaßnahmen wird man nicht entbunden. Skeptisch sehen IT-Manager auch die Kosten. Die Cloud ist längst nicht so kosteneffektiv wie versprochen.

In Sachen Cloud bleibt sich Deutschland treu und folgt nicht den einschlägigen Analystenmeinungen: »Sowohl Anwender, die bereits Cloud-Anwendungen für Backup nutzen, als auch Administratoren, die über den Gang in die Cloud nachdenken sind zunehmend skeptisch«, sagt **Albrecht Hestermann**, Leiter Vertrieb, Marketing & Produkt-

Vorteile von Cloud-Storage

1. **Skalierbarkeit:** Cloud-Speicher ermöglicht es Unternehmen, ihre Speicher-Ressourcen nahtlos zu skalieren, um sich an steigende Datenmengen anzupassen, ohne dass eine erhebliche Vorabinvestition in physische Hardware erforderlich ist.
2. **Zugänglichkeit und Zusammenarbeit:** Auf Daten in der Cloud kann von überall aus und von verschiedenen Geräten zugegriffen werden, was die Zusammenarbeit in Echtzeit ermöglicht und geografische oder zeitliche Beschränkungen minimiert.
3. **Disaster-Recovery und Datensicherung:** Cloud-Storage bietet verbesserte Optionen für die Datensicherung und Disaster-Recovery-Pläne. Daten können an mehreren geografischen Standorten repliziert werden, was die Resilienz gegenüber lokalen Ausfällen erhöht.
4. **Kosteneffizienz:** Die Nutzung von Cloud-Speicher kann zu einer Reduzierung der Gesamtbetriebskosten führen, da die Notwendigkeit für Wartung und Aktualisierung eigener Speicherinfrastrukturen entfällt und Zahlungsmodelle oft nutzungsbasiert sind.
5. **Automatisierte Updates und Wartung:** Cloud-Service-Provider kümmern sich um die Wartung des Speichersystems, inklusive regelmäßiger Software-Updates und Sicherheitspatches, was die IT-Last für Unternehmen verringert.

Nachteile von Cloud-Storage

1. **Abhängigkeit von Internetverbindung:** Der Zugriff auf Cloud-gespeicherte Daten erfordert eine stetige und schnelle Internetverbindung. Bei Ausfall oder langsamer Verbindung können Produktivitätsverluste entstehen.
2. **Sicherheitsbedenken:** Obwohl Cloud-Storage häufig fortgeschrittene Sicherheitsmaßnahmen bietet, bleibt das Risiko von Datenschutzverletzungen, vor allem bei sensiblen Daten, ein kritisches Thema.
3. **Compliance und rechtliche Bedenken:** Unternehmen müssen sicherstellen, dass ihre Cloud-Storage-Lösungen mit lokalen und internationalen Datenschutzgesetzen und Compliance-Standards übereinstimmen, was komplex sein kann.
4. **Kostenkontrolle:** Während Cloud-Storage kosteneffizient sein kann, können die Gesamtkosten unerwartet ansteigen, insbesondere bei unvorhergesehenem Datentransfer und Speichernutzung.
5. **Leistungsvariabilität:** Die Performance kann je nach Provider, ausgewähltem Service-Level und Netzwerkbedingungen variieren, was zu Inkonsistenzen in der Anwendungsleistung führen kann.

marketing bei **actidata Storage Systems**. »Insbesondere die Vertragsbindung über die Subscription-Angebote der Hersteller wird eher negativ als knebeln angesehen. Hier wird oft nach Alternativen gesucht, die einerseits in lokalen Systemen zu finden sind, aber auch in konsequent durchdachten, regionalen Cloud-Anwendungen.«

Thomas Muggendobler, Senior Product Manager Datacenter Solutions bei **Thomas-Krenn**, sieht es ähnlich: »Wir verzeichnen vermehrt Anfragen und Konzepte, die auf eine Art ‚Cloud-Exit' hinauslaufen. Das liegt auch an der komplexen Preisbildung bei den großen Hyperscalern. Gerade für kleine und mittlere Unternehmen ist das nur schwer zu durchschauen und wird schnell zur Kostenfalle. Wir merken diesen Trend bei der Nachfrage nach hybriden Infrastrukturen. Die Hardware führen wir naturgemäß und Beratungsleistungen sowie Partnerschaften haben wir entsprechend gestärkt.«

Wie gesagt, dass ist nicht die Meinung, der großen Marktbeobachter und auch die großen Storage-Hersteller brüsten sich mit der Anbindung an die Hyperscaler, **Amazon**, **Google** und **Microsoft**, inklusive der entsprechenden Zertifizierungen. Hinter vorgehaltener Hand bestätigen uns aber auch Mitarbeiter der A-Brands, dass im DACH-Raum kundenseitig das Thema Cloud weit weniger stark forciert wird, als beispielsweise in den USA.

Letztendlich ist es eine Abwägung, im jeweiligen Einzelfall. Unvorhergesehene Datentransfers können richtig ins Geld gehen. Gleichzeitig wird die hauseigene IT von Updates- und Wartungsarbeiten entlastet. Wichtig ist, die Abhängigkeit vom Internet mit einzukalkulieren und trotz aller Maßnahmen der Anbieter, es bleiben Sicherheitsbedenken. ■

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

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

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

speicherguide.de hat alle Angaben nach bestem Wissen und Gewissen geprüft, übernimmt jedoch keine Garantie über Vollständigkeit und Richtigkeit.

Fachhändler für Storage-Systeme

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

System-Pro
Altforweilerstraße 12a, 66740 Saarlouis
Tel. 068 31/12 24 62
mail@system-pro.de, www.system-pro.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,
inneo@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

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

Netzwerk Software GmbH
Einsteinring 28, 85609 Aschheim
Tel. 089/45 24 52-0,
Fax 089/452 45 24 99
info@netzwerk.de,
www.netzwerk.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
Wilhelmstraße 16-18, 91413 Neustadt/Aisch
Tel. 091 61/872 81 80, Fax 091 61/872 81 39
info@hws-gruppe.de,
www.hws-infosysteme.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

speicherguide.de hat alle Angaben nach bestem Wissen und Gewissen geprüft, übernimmt jedoch keine Garantie über Vollständigkeit und Richtigkeit.

it-daily.net

mehr als nur tägliche IT-News!

Container: skalierbar, flexibel und robust, aber auch ein Sicherheitsrisiko

BEI DER CONTAINER-NUTZUNG DIE SICHERHEIT NICHT VERGESSEN

Peter Marwan
speicherguide.de

Um sich Wettbewerbsvorteile zu verschaffen, wollen Unternehmen verstärkt hoch skalierbare, flexible, und belastbare Anwendungen haben. Die hoffen sie durch Nutzung cloud-nativer Technologien wie Kubernetes und auf Microservices basierenden Anwendungsarchitekturen zu bekommen. Aber die neue Welt stellt ihre ganz eigenen Anforderungen an die Sicherheit – die oft nicht ausreichend berücksichtigt werden.

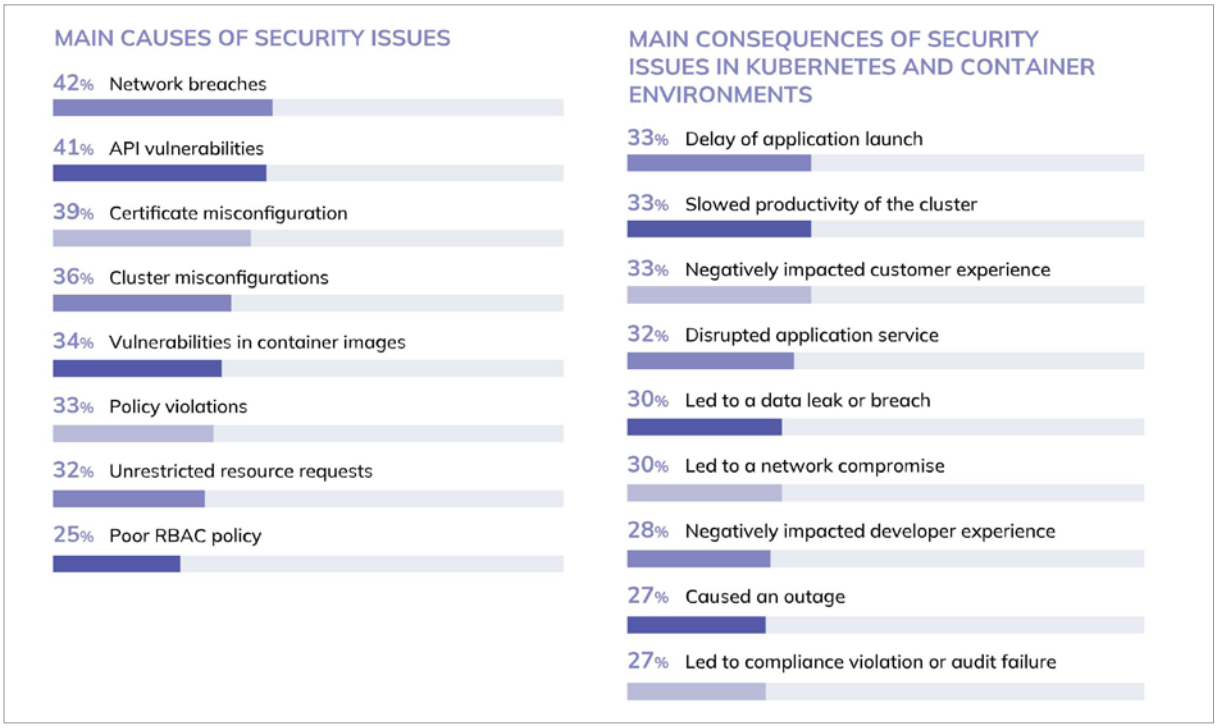
Bild: DALL-E

Mehr als die Hälfte der deutschen Organisationen hatte schon Sicherheitsprobleme in *Kubernetes* und mit der Nutzung von Containern. Das geht aus einer aktuellen Studie von **Venafi**, einem Spezialisten für das Management von Maschinenidentitäten, hervor. Zwei Drittel der insgesamt 800 Befragten fürchten, dass diese künftig noch häufiger auftreten.

Das ist nicht verwunderlich. Von den Befragten glauben 84 Prozent, dass Kubernetes bald die wichtigste Plattform für die Entwicklung ihrer Anwendungen sein wird. Und um die Sicherheit einer Plattform mit so großer Bedeutung müssen sich die Verantwortlichen natürlich Gedanken machen. Allerdings war das in der Vergangenheit nicht immer der Fall. 68 Prozent der Befragten in Deutschland, die eine Cloud-Migration durchgeführt haben, räumten ein, dass sie sich der Sicherheitsrisiken nicht bewusst waren. Zu ähnlichen Ergebnissen kam bereits im Frühjahr 2023 der »State of Kubernetes Security Report 2023« von **Red Hat**.

Container haben ihre eigenen Tücken

Ein Grund dafür könnte sein, dass die meisten (88 Prozent) damit begonnen haben, Legacy-Anwendungen in die



Grafik: Venafi

Venafi hat 800 Verantwortliche zu den Gründen und den Konsequenzen für Sicherheitsproblem mit Containern und Kubernetes befragt

Cloud zu verlagern. Über die Hälfte davon hat es dabei jedoch versäumt, diese Anwendungen mit nativen Cloud-Technologien auch neu zu strukturieren. Die Software läuft also lediglich auf anderen Servern. Angepasst wurde sie kaum oder gar nicht – denn das wäre ja aufwändig und langwierig gewesen. Allerdings verschenken sie so nicht nur einiges des eigentlichen Potenzials der Cloud, sondern riskieren auch in die eine oder andere Sicherheitsfalle zu tappen.

Immerhin steigt das Bewusstsein dafür: Drei Viertel der von Venafi befragten befürchten, dass die Geschwindigkeit und Komplexität von Kubernetes und Containern zu neuen Sicherheitslücken führt.

90 Prozent sind der Meinung, dass sie mehr Know-how für native Cloud-Umgebungen aufbauen müssen, um die Sicherheit ihrer Anwendungen zu gewährleisten. Oft rührte die Einsicht allerdings daher, dass es bereits einmal gebrannt hat: 77 Prozent der Befragten aus Deutschland (nur 59 Prozent weltweit) hatten bereits mit Sicherheitsproblemen in ihren Kubernetes- oder Container-Umgebungen zu kämpfen. Die häufigsten Ursachen waren Netzwerkprobleme, API-Schwachstellen und Fehlkonfigurationen von Zertifikaten.

»Cloud Native ist der Weg in die Zukunft und ermöglicht äußerst skalierbare, flexible und robuste Anwendungen, die einen Wettbewerbsvorteil bieten können«, sagt **Matt Barker**, Global Head of Cloud Native Services bei Venafi. Seiner Ansicht nach basieren daher in ein paar Jahren voraussichtlich die meisten Anwendungen auf einer Cloud Native Architektur. »Allerdings neigen viele Unternehmen dazu, den erforderlichen Aufwand für Effizienz und Sicherheit zu unterschätzen. Mit dem zunehmenden Verschieben kritischer Arbeitslasten in cloud-native Umgebungen ist es entscheidend, diese Lücken zu schließen, da andernfalls weitere Sicherheitsverletzungen und Ausfälle auftreten könnten.«

Laut Matt Barker, Global Head of Cloud Native Services bei Venafi neigen viele Unternehmen dazu, bei Containern den Aufwand für Effizienz und Sicherheit zu unterschätzen.

Bild: Venafi

Schlankere Container-Images mit weniger Angriffsfläche

Mit dieser Erkenntnis steht Barker nicht allein. So kündigte zum Beispiel auf der »DockerCon« Anfang Oktober **Sysdig** eine Partnerschaft mit **Docker** an. Ziel ist es, durch die Kombination von *Sysdig RuntimeInsights* mit *Docker Scout* die Bereitstellung von

»In großen Firmen ist das Thema Container-Sicherheit schon angekommen.«

Denis Maligin und Stefan Buchberger, Sysdig

Bild: Peter Marwan

Cloud-nativen Anwendungen zu beschleunigen und zu sichern. Das soll Entwicklern helfen, Risiken zu priorisieren und »Software Supply Chain Noise« zu reduzieren – also schlankere Container-Images zu erstellen und indem unnötiger Code vermieden wird, auch weniger Angriffsfläche zu bieten.

Sysdig ist Anbieter einer Cloud-native Plattform für den Schutz von Anwendungen (CNAPP) – sowie das unter anderem auch **Check Point Software**, **Crowdstrike**, **Microsoft**, **Palo Alto Networks**, **Trend Micro** oder **Zscaler** für sich in Anspruch nehmen. Vom Wettbewerb hebt sich Sysdig eigenen Angaben zufolge ab, weil es Einblicke während der Laufzeit der Anwendungen nutzt, statt eher statischer Analysen. So sollen sich Schwachstellen und Berechtigungen in der Anwendung und Multi-domain-Korrelation über den gesamten Software-Lebenszyklus hinweg identifizieren lassen.

Docker Scout liefert Entwicklern zusätzlich kontextbezogene Empfehlungen. Sie können so sicherstellen, dass sie sicherere Images ausliefern. Die Integration mit der *Docker Build-and-Push-GitHub-Action* hilft zudem, die Übertragung riskanter Images zu vermeiden.

Außerdem soll das Tool bei der Priorisierung der Schwachstellenbehandlung helfen: Laut Sysdig lasse sich der »Monitoring Noise« um bis zu 95 Prozent reduzieren, indem ermittelt wird, welche Schwachstellen ausgenutzt werden und welche nicht. »Indem wir sichtbar machen, welche Pakete in der individuellen Konfiguration überhaupt verwendet werden, helfen wir den Entwicklern Prioritäten setzen und schneller sichere Software zu liefern«, erklärt **Stefan Buchberger**, Marketing Manager CEMEA bei Sysdig.

Am Beispiel der Abwehr einer Bedrohung wie »SCARLETEEL« lässt sich Sysdig zufolge der Nutzen der Container-Überwachung zur Laufzeit gut aufzeigen. Mit dem Angriff wird seit Anfang 2023 versucht, AWS-Konten zu kompromittieren, Daten zu klauen und Krypto-Mining durchzuführen. Sysdig beobachtete zudem, dass auch Kubernetes ins Visier genommen wurde, um den Angriff erheblich auszuweiten. »Die Erkennung von Bedrohungen zur Laufzeit und die Reaktion darauf sind entscheidend, um zu verstehen, wann ein Angriff stattgefunden hat, Werkzeuge wie Schwachstellen-Management, CSPM und CIEM könnten diese Angriffe verhindern«, sagt Buchberger.

»Im Mittelstand herrscht viel Bedarf für Container-Sicherheit – bisherige Angebote sind aber oft zu komplex.«

Waldemar Bergstreiser, Kaspersky

Bild: Peter Marwan

Neu im Markt: Kaspersky Container Security

Neben Spezialisten wie Sysdig bieten aber auch immer mehr klassische IT-Security-Anbieter Produkte zur Container-Absicherung an. Jüngstes Beispiel ist *Kaspersky Container Security*. Die Lösung soll containerisierte Anwendungen von der Entwicklung bis zum Einsatz absichern, sei »direkt nach der Installation einsatzbereit, kostengünstig und leicht in die IT-Infrastruktur eines Unternehmens integrierbar«, erklärt der Hersteller.

Auch Kaspersky verspricht Schutz zur Runtime, beispielsweise indem nur der Start vertrauenswürdiger Container erlaubt und der Betrieb von Anwendungen und Diensten innerhalb der Container gesteuert sowie der Datenverkehr überwacht werden. Dazu prüft *KCS Scanner* die Konfigurationsdateien auf Fehlfunktionen und scannt Images auf Schwachstellen, Malware und vertrauliche Daten. Außerdem überprüft er die Übereinstimmung mit Richtlinien innerhalb der Image-Registry und CI/CD-Plattformen.

KSC Agent schützt vor Angriffen auf die Anwendung im Container, überwacht die Interaktion von Containern und Netzwerken in Clustern und überprüft das Gesamtsystem auf die Einhaltung von Sicherheitsstandards.

Der *KSC Server* schließlich aggregiert die vom Scanner und Agenten erhaltenen Daten, bereitet die Daten visuell auf und hilft beim Reporting und Berichten sowie der Interaktion mit anderen Security-Plattformen – unter anderem Kasperskys hauseigenem SIEM. ■

”Unternehmen denken nach, Thought Leader denken voraus!”

Technische Perspektiven und Herausforderungen

PRIMÄRSPEICHER: KERN DER IT-INFRASTRUKTUR

Karl Fröhlich
speicherguide.de

Michael Baumann
speicherguide.de

Primärspeicher, auch als Primary-Storage bekannt, ist entscheidend für den Betrieb und die Effizienz von IT-Systemen in Unternehmen jeder Größe. Moderne Primärspeichersysteme müssen eine Vielzahl von Anforderungen erfüllen, einschließlich hoher Performance, Zuverlässigkeit, Skalierbarkeit und Sicherheit.

In der modernen IT-Landschaft ist der Primärspeicher das Herzstück der Datenspeicherung, von Rechenzentren bis hin zum Netzwerkrand (Edge). Noch sind Hybrid-Systeme im Einsatz, die sowohl SSDs als auch HDDs nutzen, die Zukunft gehört aber All-Flash-Arrays (AFAs).

All-Flash bietet im Vergleich zu Hybrid-Speichern signifikant höhere Geschwindigkeiten. Dies ist besonders wichtig für Anwendungen, die bei vielen Nutzern im ständigen Zugriff stehen bzw. schnelle Lese- und Schreibvorgänge erfordern. Zudem sind sie energieeffizienter und benötigen weniger Stellfläche. Anbietern zufolge sind AFAs einfacher zu verwalten, da sie keine Disk- und Flash-Tiering-Mechanismen benötigen. Da Flash-Speicher ohne bewegliche Teile auskommen, gelten sie als zuverlässiger.

Im Gegensatz zu Hybrid-Systemen, die bei bestimmten Workloads Leis-

Bild: via Canva Pro

tungsschwankungen aufweisen können, bieten AFAs eine konsistentere Performance und insgesamt mehr Zukunftssicherheit: Mit dem Wechsel zu NVMe und NVMe-oF sind AFAs besser positioniert, um zukünftige Technologie-Entwicklungen zu nutzen. Laut **Exactitude Consultancy** soll der Markt für AFAs bis 2029 einen Umsatz von fast 56 Milliarden US-Dollar erreichen. Dies entspricht einem jährlichen Wachstum von durchschnittlich über 16 Prozent. Die von *speicherguide.de*-Lesern identifizierten Herausforderungen, gelten auch für den Bereich Primärspeicher: Das heißt, wachsender Speicherbedarf und hohe Investitionskosten. Für Unternehmen ist die richtige Auswahl entscheidend, zu den Kriterien gehören Performance, Zuverlässigkeit, Skalierbarkeit, Sicherheit und natürlich die Kosten.

Unserer Leserumfrage zufolge nutzen 88 Prozent File-Speicher und 50 Prozent Blockspeicher. 34 Prozent setzen auf Objektspeicher. 54 Prozent der Unternehmen kommen mit 50 TByte für Primärdaten aus, während 39 Prozent bis zu 1 PByte nutzen.

Mit All-Flash haben sich auch NVMe sowie NVMe-over-Fabrics (NVMe-oF), bei der Konnektivität für den Aufbau systemübergreifender, performanter Netzwerke durchgesetzt.

Lokal werden Primärspeicher in SAN- oder NAS-Architekturen betrieben. Übergreifende Betriebssystem-Software spielt beim Einsatz von lokalem Primärspeicher unterschiedlicher Klassen auch im Zusammenspiel mit Cloud-Kapazitäten eine Rolle. In vielen Lösungen sollen zudem Software-definierte Ansätze helfen, den Einsatz von Primärspeicher effektiv zu gestalten.

Primärspeicher: Die wichtigsten Grundlagen

Bei der Auswahl eines Primärspeichers sollten IT-Manager folgende Kriterien abfragen:

1. Kontinuierlicher Geschäftsbetrieb: Die Lösung der Wahl muss in der Lage sein, Datenredundanz lokal und über Remote-Standorte zusammen mit Spiegelungs- integrierten Failover-, Resynchronisations- und Failback-Funktionen zu schaffen. Darüber hinaus sollten zeitpunktbezogene Datenwiederherstellungstechniken (Snapshots, Backup-Integration, eventuell CDP) ent-

Hitachi Vantara

Hitachi deckt mit seinen All-Flash- und Hybrid-Systemen der *Virtual Storage Plattform VSP* (E990- , 5000-, E-, F- und G-Serie) ein breites Spektrum ab. Gemeinsam ist das NVMe-optimierte Betriebssystem *Storage Virtualization Operating System* (SVOS). Die Kunden kommen in der Regel aus den Segmenten großer und mittelständischer Unternehmen. Jüngste Neuerungen fokussierten auf Verbesserungen am auf künstlicher Intelligenz (KI) basierenden Verwaltungssystem, das Automatisierung, Analysen und Daten-Schutz bietet. Hitachi-Systeme stehen laut Gartner im Ruf, gute Performance durch fortschrittliches Caching zu bieten.

Kürzlich vorgestellt wurde die *Hitachi Virtual Storage Platform One*, laut Hersteller ein neuer Ansatz für Hybrid-Cloud-Datenspeicherung. Die Basis bildet eine einheitliche Architektur, die darauf ausgelegt ist, block-, datei-, objekt-, cloud-, mainframe- und software-definierte Speicher-Workloads möglichst effizient zu verwalten. Sie verwaltet verschiedene Datentypen und unterstützt den flexiblen Verbrauch als Appliance oder software-definiert in öffentlichen Cloud- und On-Premises-Umgebungen. Ein KI-fähiger Software-Stack verwaltet die Plattform und soll Infrastruktur-, Daten- und Anwendungssilos beseitigen.

Dell Technologies/Dell EMC

PowerStore, *PowerScale*, *PowerFlex* und *PowerMax* sind die Primärspeicher-Plattformen von **Dell**. Der All-Flash-Speicher Powerstore eignet sich besonders für geschäftskritische Transaktions-Workloads, *VMware*-Anwendungen und Datenbank-Workloads. Powerstore ist für den Midrange-Speichermarkt konzipiert und mit seiner software-definierte Infrastruktur, für 3-Tier-SAN ausgelegt sowie für hyperkonvergente Architekturen, Hochleistungs-Workload-Konsolidierung und containerisierte Apps. Powerflex, ein Multi-Hypervisor-unterstütztes SDS-Angebot, zielt auf Datenbank- und andere Transaktions-Workloads in einer Scale-out-Architektur mit linearer Leistungsskalierung. Die Powermax-Serie bezeichnet Dell als eines der weltweit sichersten Speichersysteme für unternehmenskritische Anwendungen, geeignet für Mission-Critical-Workloads, Zero-Trust-Architekturen und die Konsolidierung gemischter Workloads.

Jedes dieser Systeme bietet spezifische Vorteile für unterschiedliche Anforderungen, von hoher Performance und Sicherheit (Powermax) über Flexibilität und Skalierbarkeit (Powerflex) bis hin zu spezialisierten Lösungen für KI- und Cloud-basierte Anwendungen (Powerscale, Powerstore).

Pure Storage

Pure Storage bearbeitet mit seiner High-Performance-Lösung *FlashArray//X*, der High-Capacity-Variante *FlashArray//C* und seinen *FlashBlade*-System mit geringerer Leistung den Markt für Primary-Storage. Der Anbieter schneidet laut Gartner insbesondere im Enterprise-Segment und bei großen, globalen Unternehmen gut ab.

Flasharray//C ist die Kapazitätsversion der NVMe-Produktreihe und das erste All-QLC-Flash-Array am Markt. Performance-Spitzen und höchste Speicherdichte verspricht das Flasharray//X für geschäftskritische Enterprise-Anforderungen an die Performance. Zugrunde liegt das Betriebssystem *Purity*.

Neu hinzugekommen ist das *FlashArray//E*. Laut Pure, ist es das erste All-Flash-System, das im Einstiegssegment mit Festplattensystemen konkurrieren kann. Die Systeme richten sich an KMU-Kunden, um gängige Workloads bereits mit einer Kapazität ab einem PByte zu unterstützen.

Die Lösung verspricht einen 80 Prozent geringeren Strom- und Platzbedarf, 60 Prozent niedrigere Betriebskosten und 85 Prozent weniger Elektroschrott im Vergleich zu Festplatten.

Netapp

NetApp adressiert eine breite Palette von primären Speicher-Workloads mit seinen Arrays der *AFF*, *FAS*, *SolidFire*, *E-Series*, *EF-Series*. Netapp gilt als führend bei der Integration mit Public-Cloud-Anbietern und bei der Unterstützung von Hybrid-Cloud-IT-Infrastrukturen. Die Data-Fabric-Strategie und die den Lösungen gemeinsame *ONTAP*-Software bieten eine einheitliche Verwaltungsplattform für hybride Cloud-Speicherumgebungen.

Neu Portfolio sind drei Flash-Arrays der *ASA C*-Serie. Diese sind darauf ausgelegt, Informationen in Blockform zu speichern. Bis zu zwölf ASA-C-S-Arrays lassen sich miteinander verbinden, mit Kapazitäten zwischen 17,5 und 88 PByte zu schaffen. Die ASA C-S-Arrays sind laut Hersteller darauf ausgelegt, Geschwindigkeit mit Kosteneffizienz zu balancieren, und bieten Latenzzeiten im Bereich von zwei bis vier Millisekunden. Die Systeme sollen sich für unternehmenskritische Anwendungen eignen, Datenbanken und *VMware*-Infrastrukturen.

halten sein, um im Falle eines Datenverlusts basierend auf dem letzten bekannten »guten« Datenstatus zum normalen Betrieb zurückzukehren.

2. Schneller Datenzugriff: Die Reaktionsfähigkeit der Speichergeräte ist entscheidend für eine positive Benutzererfahrung. Folglich sollte die gewählte Lösung inhärente Funktionalitäten abdecken, um das Antwortverhalten des Speichers zu verbessern. Dies können Caching-Mechanismen, parallele Operationen und die vollautomatische, kontinuierlich aktualisierte und transparente Ablage der Daten auf dem jeweils richtigen Speicher (Auto- Tiering) sein.

3. Integration neuster Technologien: Um zukünftig Implementierungszeit und -kosten zu sparen, sollte die gewählte Lösung einfache Möglichkeiten bieten, neue Technologien einfach in die bestehende Umgebung einzubinden. Außerdem sollte es möglich sein, Speichergeräte während des Geschäftsbetriebs hinzuzufügen, auszutauschen oder außer Betrieb zu nehmen.

4. Unterbrechungsfreie Datenmigration: Die Migration von Daten ist ein komplexer Prozess, der enorme Anstrengungen erfordert und einige Risiken birgt. Daher sollte die Lösung eine nahtlose Migration von Daten zwischen allen unterschiedlichen Speichermedien ermöglichen, ohne dass es zu Beeinträchtigungen des Tagesgeschäfts kommt.

5. Automatisiertes Management der Speicherdienste: Damit IT-Teams produktiver arbeiten können, müssen sie davon befreit werden, zu viel Zeit mit unwichtigen Aufgaben zu verbringen. Der einfachste Weg, dies zu erreichen, ist Automatisierung. Lösungen sollten dabei massiv helfen, sich wiederholende manuelle Verwaltungsaufgaben zu automatisieren.

6. High-End-Datendienste und Kapazitätsmanagement zentralisieren: Es sollten Lösungen bevorzugt werden, die Ressourcen über verschiedene Speicher-Hardware hinweg aggregieren können, idealerweise unabhängig davon, wie sie physisch verbunden sind, und die Kapazitätsbereitstellung und Lastverteilung zentral verwalten.

7. Scale-up- oder Scale-out-Skalierung: Unabhängig davon, ob lokale Speicherumgebungen Scale-up oder Scale-out skaliert werden, oder mit einer Hybrid-Cloud-Strategie angebunden sind, muss die Lösung Möglichkeiten zur Kapazitätserweiterung bieten, um heutigen und zukünftigen Anforderungen gerecht zu werden.

8. Flexible Lizenzierung: Transparente Lizenzierung und wettbewerbsfähige Preise sollten geboten werden, speziell wenn der Kapazitätsbedarf wächst. Die meisten Hersteller haben entsprechende On-Demand-Angebote im Portfolio. ■

Fujitsu

Das Produktportfolio von **Fujitsu** besteht aus Storage *ETERNUS AF DX* (All Flash) und *ETERNUS DX* Hybrid-Systemen. Sie decken das Einstiegs-, Mittelstands- und Enterprise-Segment ab. Bereits seit 2020 vertreibt Fujitsu, im Rahmen einer OEM-Vereinbarung mit **NetApp** auch *NetApp AFF*– und *FAS*-Systeme in Europa.

Eternus DX- und AF-Midrange-Produkte bieten dedizierte Speicherbeschleunigungs-Engines und NVMe-basierten Lese-Cache. Sie gelten als preislich günstiger im Vergleich zu vielen Wettbewerbern bei, laut **Gartner**, allgemein hoher Kundenzufriedenheit.

DDN (Data Direct Networks)

DDN entwickelt seine High-Performance-Computing-Technologien (HPC) insbesondere Speicher-seitig. So unterstützt die *VMstore*-Plattform NVMe und basiert auf der hauseigenen *IntelliFlash*-

Betriebssystem-Plattform. DDN Vmstore soll intelligente Einblicke in die Speicherinfrastruktur ermöglichen, AIOps (Artificial Intelligence for IT Operations) und Analysen, proaktives Input-Output-Management und optimierte Ressourcenzuweisung für optimierte Performance, für die der Hersteller steht

DDN hat kürzlich die *Infinia*-Plattform eingeführt, eine software-definierte Speicherlösung der nächsten Generation. Diese Plattform ist darauf ausgelegt, in komplexen Workflows Mehrwert zu schaffen, insbesondere in den Bereichen Enterprise AI und Cloud-Anwendungen. Zu den Schlüsselfunktionen von DDN Infinia sollen Multi-Tenancy, eine verbesserte Verwaltung, Sicherheit und Effizienz gehören. Die neuen Systeme sind laut Hersteller für ein beschleunigtes Computing und generative KI ausgelegt.

Lesen Sie den Artikel in einer detaillierteren Langfassung auf **speicherguide.de**

”Unternehmen denken nach, Thought Leader denken voraus!”

Cybersicherheit, Digitalisierung und demografischer Wandel fordern mehr Personal

IT-FACHKRÄFTEMANGEL: EFFIZIENZ UND RECRUITING ALS SCHLÜSSEL

Karl Fröhlich
speicherguide.de

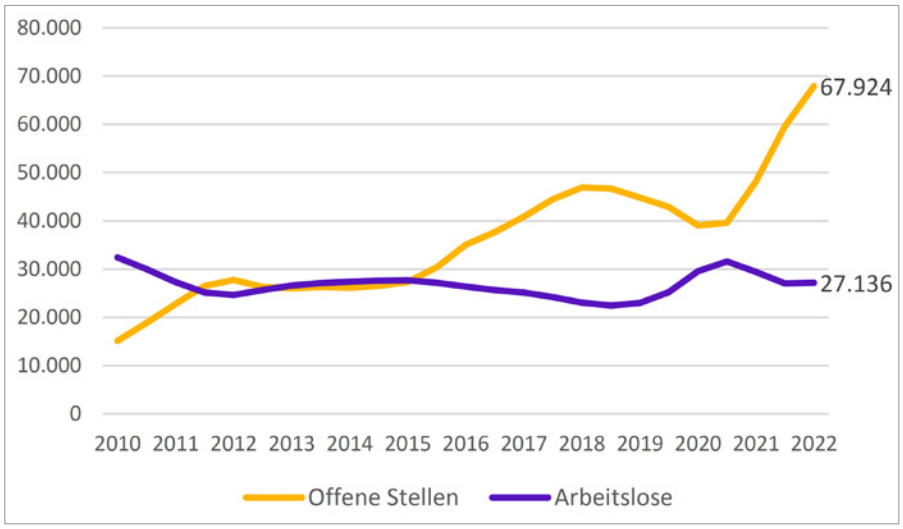
Bei allen technischen Anforderungen, es fehlt oft genug am nötigen Personal, welches für die Umsetzung sorgt. Mittlerweile gibt es eine wachsende Diskrepanz zwischen Bedarf und Verfügbarkeit von qualifizierten IT-Fachkräften. Für Firmen heißt das, die Effizienz der IT zu steigern und mehr in Recruiting-Strategien zu investieren.

In nahezu allen Gesprächen hören wir in der *speicherguide.de*-Redaktion von ein und demselben Problem, das interessanterweise gar nicht so viel mit Technik zu tun hat, sondern dem Mangel an IT-Fachkräften. Dies gilt für IT-Abteilungen, Systemintegratoren, Distributoren und Hersteller gleichermaßen.

»Dieses Problem wird sich aus mehreren Gründen auch künftig weiter zuspitzen«, erwartet **Marius Neidlinger**, Business Development Manager bei **Dell Technologies Deutschland**. »Einerseits stehen durch den demographischen Wandel viele Fachleute kurz vor dem Ruhestand, während aufgrund der zunehmenden Digitalisierung der Bedarf an IT-Spezialisten in den Unternehmen rasant ansteigt.«

Dem **Institut der deutschen Wirtschaft** (IW) zufolge hat der Fachkräftemangel in IT-Berufen 2022 mit 68.000 offenen Stellen einen neuen Höchststand erreicht. Der hohe Bedarf an qualifizierten Fachkräften fällt auch mit einem Rückgang der Absolventenzahlen an den Hochschulen zusammen. Der Digitalverband **Bitkom** spricht in seiner Studie zum IT-Fachkräftemangel von 137.000 offenen IT-Stellen.

Laut einer **ifo** Konjunkturumfrage bei etwa 9.000 Unternehmen aus ganz Deutschland leiden im Sommer 2023 rund 43 Prozent der Firmen unter Engpässen an qualifizierten Arbeitskräften.



Offene Stellen und Arbeitslose in IT-Berufen

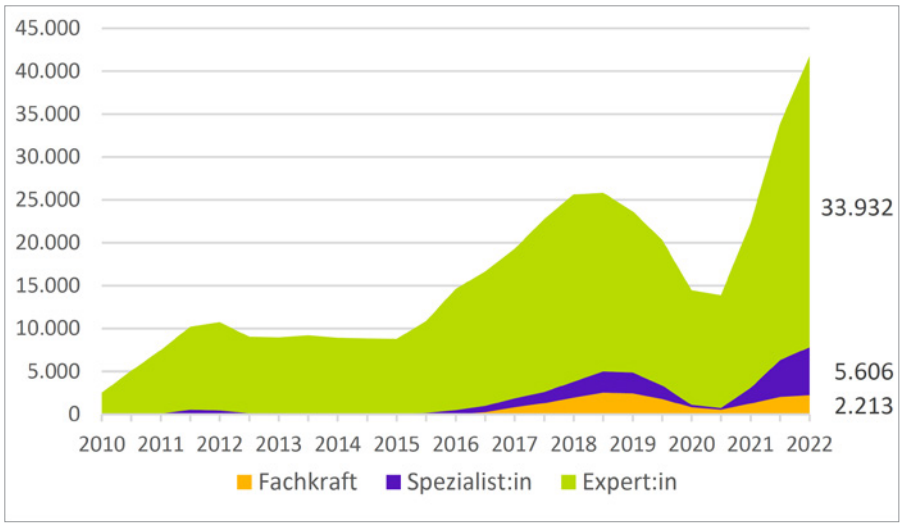
Quelle: KOFA-Berechnungen auf Basis von Sonderauswertungen der BA und der IAB-Stellenerhebung, 2023

Personalmangel mit Technik entgegenwirken

»Die wachsenden Anforderungen an die IT bei gleichzeitig sinkenden personellen Ressourcen können kurz- und mittelfristig nur durch massive Effizienzsteigerungen bei der Bereitstellung und dem Betrieb der IT gelöst werden«, sagt Dell-Manager Neidlinger. »Dies erfordert eine Kombination aus Automatisierung und Konsolidierung bei gleichzeitiger Verringerung der Komplexität. Technologisch erreicht man das durch die Vermeidung von Silos sowie einer konsequenten Standardisierung im Bereich der Soft- und Hardware. Appliance-basierte und Software-definierte Ansätze sind hier ein bevorzugtes Mittel der Wahl.«

Recruiting: Unternehmen müssen Aufwand erhöhen

Unternehmer und Vertriebsexperte **Dirk Kreuter** hält den Fachkräftemangel eher für einen Mythos. Vielmehr betreiben Firmen nicht genug Aufwand, um gute Mitarbeiter zu bekommen. »Der Prozess neue Mitarbeiter zu gewinnen, ist der gleiche, wie neue Kunden zu gewinnen«, stellt Kreuter klar. Kreuter hat im vergangenen Jahr 220.000 Euro für Recruiting-Maßnahmen ausgegeben, im gleichen Zeitraum aber 5,8 Millionen Euro für Werbung. »Diesen Denkfehler habe ich auch erst kürzlich für mich aufgelöst«, erklärt Kreuter. »Geld für Neukunden



Die Entwicklung der Fachkräftelücke in IT-Berufen nach Qualifikation: Anzahl an offenen Stellen, für die es keine passend qualifizierten Arbeitslosen gibt.

Quelle: KOFA-Berechnungen auf Basis von Sonderauswertungen der BA und der IAB-Stellenerhebung, 2023

habe ich immer gerne ausgegeben, Geld für neue Mitarbeiter, da habe ich immer auf der Bremse gestanden. Bis Mitte 2023 haben wir bereits mehr Geld für Recruiting ausgeben als im Gesamtjahr 2022. Dadurch hat sich die Anzahl der Bewerber deutlich erhöht und auch deren Qualität.« Sein Kredo, wer gute Mitarbeiter haben möchte, muss auch an der Stelle investieren, um mehr A+-Mitarbeiter zu bekommen, die für das Unternehmen Leistung bringen und entsprechende Erfolge einfahren.

Marktbeobachter wie **Andreas Raum**, Geschäftsführer bei **freyraum marketing**, ergänzt: »Der Fachkräftemangel ist ein Arbeitskräftemangel, kein Mythos, sondern wird schnell schlimmer. Ansonsten sehe ich es genauso, Unternehmen müssen gegensteuern und dies massiv.«

Firmen und potenzielle Mitarbeiter sollten sich aufeinander zubewegen

Allerdings gibt es auch kritische Stimmen, die Unternehmen vorwerfen, nicht genug in Aus- und Weiterbildung zu investieren. Zudem würden viele schlicht keine angemessenen Gehälter und Arbeitsbedingungen bieten. Das ist sicherlich ein diskussionswürdiger Punkt. Das Gegenargument lautet meist, die Neuen müssen sich in das bestehende Gehaltsgefüge einfügen. Man könne ja nicht allen bei jeder Neueinstellung das Gehalt erhöhen.

Letztendlich sind nicht alle Unternehmen gleich und viele müssen sich noch an die neuen Gegebenheiten anpassen. Die jüngere Generation hat heute höhere Ansprüche, die eingesessene Firmenlenker oft genug als maßlos überzogen halten. Am Ende werden sich beide Seiten aufeinander zu bewegen müssen. Und es ist ja nicht neu, dass man gut ausgebildeten Fachkräften etwas bieten muss um sie zu bekommen bzw. zu halten. Das Gehalt ist ein Faktor, aber jeder mit etwas Berufserfahrung achtet vor allem auf das Arbeitsklima.

Arbeitsklima entscheidend

Dies beginnt beim Führungsstil und der Art und Weise, wie Vorgesetzte mit ihren Mitarbeiterinnen und Mitarbeitern umgehen. Die Kommunikation sollte offen und klar sein und die Arbeit wertgeschätzt und anerkannt werden. Und dies bei allen und nicht nur ausgewählte Kolleginnen und Kollegen. Gute Chefs beziehen ihre Mitarbeitenden in Entscheidungsprozesse mit ein und geben ihnen ein Gefühl der Wertschätzung und Zugehörigkeit.

Die Faktoren sind vielfältig, oft nicht greifbar und insgesamt ein komplexes Konstrukt. Auch kommen diverse Maßnahmen nicht bei allen gleich gut an. Während die einen gerne Weiterbildungen und Teambuilding-Maßnahmen besuchen, sind sie für andere die Hölle. Experten raten zu einem aktiven Management, mit einem guten Verständnis und Gespür für die Teamdynamik. Müssen unliebsame Entscheidungen getroffen werden, gilt es diese klar zu kommunizieren und nicht aufzuschieben.

IT-Fachkräfte: Entwicklung in den kommenden zwölf Monaten

Die steigende Zahl an Cyberattacken forciert den Bedarf an Sicherheitsspezialisten und Forensiker. Hinzukommt der Durchbruch im Bereich Künstlicher Intelligenz (KI), die zusätzliche Software-Entwickler für das Design, die Implementierung und die Wartung von KI-Systemen benötigen. Hinzukommen Datenwissenschaftler und Datenanalytiker, sie füttern die KI mit Daten und analysieren die Ergebnisse, um daraus Erkenntnisse für die Unternehmen zu gewinnen.

Die wirtschaftliche und politische Entwicklung bleibt auf absehbare Zeit ein Hemmschuh, denn zu den Auswirkungen der Pandemie kommen wirtschaftliche Schwankungen. Erst wenn sich die Lage stabilisiert, werden Unternehmen ihre IT-Projekte wieder stärker vorantreiben.

Gleichzeitig schreitet die Digitalisierung in allen Wirtschaftssektoren, Behörden und Gemeinden voran. Zum Teil sehr langsam, aber stetig. Wie sehr Spezialisten fehlen, zeigt sich in mehreren Gemeinden, Behörden, Städten und Kliniken, die nach einem Ransomware-Angriff auf unbestimmte Zeit von der normalen IT abgeschnitten sind. ■

Lesen Sie den Artikel in einer detaillierteren Langfassung auf **speicherguide.de**