

The background of the top half of the slide is a photograph of the modern glass and concrete facade of the Universitätsklinikum Dresden. Large glass windows reflect the sky and surrounding trees. A semi-transparent white box is overlaid on the left side of the image, containing text.

Universitätsklinikum Dresden

AUFWANDSREDUKTION UND ZUKUNFTSSICHERHEIT

WENIGER AUFWAND UND MEHR ZEIT FÜR Kernaufgaben

„Dank der Architektur von iCAS FS haben wir seit der Umstellung noch weniger Aufwand mit Archiv und Storage. Seit Abschluss der Datenmigration haben wir die Verantwortung dafür fast vollständig an iTernity abgegeben.“

Andreas Naumertat,
Teamleiter Server/Storage/Backup, Universitätsklinikum Dresden (UKDD)

UNIVERSITÄTSKLINIKUM DRESDEN UKDD

Branche:

Gesundheitswesen

Ausgangslage:

Im UKDD wachsen die Datenmengen rasant. Diese Daten müssen hochverfügbar und nach strengen Richtlinien und Sicherheitsstandards gespeichert werden. Als die Modernisierung der eingesetzten Speicherlösung anstand, wünschte sich das UKDD eine flexible und effiziente Lösung mit klarem Fokus auf Ransomware-Schutz und einem hohem Service-Level.

Herausforderungen:

- Speicherung und Schutz sensibler medizinischer Daten nach strengen Vorgaben
- Zukunftssicherheit durch Skalierbarkeit und Kosteneffizienz
- Nahtlose Integration in die bestehende Infrastruktur
- Management und Administration des Datenspeichers sollten ausgelagert sein

Lösung:

iCAS FS Speicherplattform von iTernity
HYDMedia und DeepUnity von Dedalus

Bild (Universitätsklinikum Dresden): Das Universitätsklinikum Dresden ist das einzige Krankenhaus der Maximalversorgung in Ostsachsen.

DER ERFOLG AUF EINEN BLICK



Kein Aufwand für das UKDD mit der Speicherplattform: Administration, Monitoring, Updates & Betrieb erfolgen durch iTernity



WORM-Speicherung, Ransomware-Schutz und Ausfallsicherheit garantieren die Sicherheit, Integrität und Verfügbarkeit der Daten



Bewältigung des Datenwachstums mithilfe der Scale-out Speicherplattform iTernity iCAS FS



Von den Vorzügen der Public Cloud im eigenen Rechenzentrum profitieren

SENSIBLE GESUNDHEITSDATEN SICHER IN DIE ZUKUNFT BRINGEN

Wie können wir unsere sensiblen medizinischen Daten auch zukünftig gegen Verlust und Manipulation absichern, das Datenwachstum bewältigen und dabei Kosten und vor allem Zeit einsparen?

Diese Frage stellten sich die IT-Verantwortlichen des Universitätsklinikums Carl Gustav Carus Dresden (UKDD) im Jahr 2020 als das bisherige Speichersystem neu aufgestellt werden sollte.

Das Universitätsklinikum Dresden ist eines der größten Krankenhäuser Sachsens und zugleich das einzige Krankenhaus der Maximalversorgung in Ostsachsen. Es verfügt über 1.410 Betten und 201 tagesklinische Behandlungsplätze. Die Dresdner Hochschulmedizin ist führend in der Behandlung komplexer, besonders schwerer oder seltener Erkrankungen. So genießt das UKDD einen sehr guten Ruf in der Behandlung und Erforschung des Diabetes mellitus Typ 1 und Typ 2 sowie seiner Folgeerkrankungen, und ist eine der führenden Kliniken in der Behandlung von Krebserkrankungen sowie neurologischen Erkrankungen. Pro Jahr werden über 53.000 Patient:innen stationär und knapp 165.000 Patient:innen ambulant behandelt.

Für die IT des UKDD ist das Datenmanagement ein sensibler Prozess, da es sich um eine große Menge unterschiedlichster kritischer Gesundheitsinformationen aus einer Vielzahl von Quellen mit Aufbewahrungsfristen von bis zu 30 Jahren handelt. Diese Daten müssen besonders geschützt werden, dürfen nicht verändert oder manipuliert werden und müssen nach strengen Vorgaben aufbewahrt werden. Zudem ist aufgrund der Akutbehandlung ein schneller Zugriff auf die Archivdaten elementar und die Hochverfügbarkeit kritisch für die Patientenversorgung.

Erschwerend kommt hinzu, dass die Datenmengen rasant wachsen und ein lukratives Ziel für Ransomware-Attacken darstellen. Die Abteilung Basisinfrastruktur des UKDD ist mit ca. 20 Mitarbeiter:innen (sechs davon zuständig für den Bereich Server/Storage/Backup) zwar gut aufgestellt, der zunehmende Fachkräftemangel macht sich jedoch auch hier deutlich bemerkbar.

Für die IT-Verantwortlichen des UKDD stellten sich daher folgende Kernfragen:

- Welche Lösung fügt sich nahtlos in die bestehende IT-Landschaft ein und bietet effektiven Support zur Entlastung der klinischen IT?
- Wie können Daten aus bildgebenden Verfahren – wie Röntgenbilder und medizinische Befunde – langfristig, hochverfügbar und sicher gespeichert werden?
- Wie lassen sich die gespeicherten Daten noch besser vor Ransomware-Attacken schützen?
- Wie können Effizienz, Skalierbarkeit und Flexibilität weiter optimiert werden, um mit den rasant wachsenden Datenmengen Schritt zu halten?



Eckdaten: UKDD

- Universitätsklinikum
- Stationäre und ambulante Krankenversorgung, Therapie komplexer, besonders schwerer oder seltener Erkrankungen
- Über 53.000 stationäre und 165.000 ambulante Patient:innen pro Jahr
- Etwa 6.770 Mitarbeiter:innen

SICHERHEIT, PERSONALKNAPPHEIT UND DATENWACHSTUM

Im Jahr 2015 entschieden sich die IT-Verantwortlichen des UKDD, die zuvor für die Datenspeicherung eingesetzte proprietäre Netzwerkspeicherplattform, die in die Jahre gekommen war, durch die Archiv-Middleware iCAS von iTernity zu ersetzen.

Seitdem setzt das UKDD erfolgreich auf iCAS zur sicheren und Compliance-konformen Archivierung sensibler Daten aus den Systemen HYDMedia und DeepUnity der Dedalus Healthcare Group. HYDMedia ist ein ganzheitliches Enterprise Content Management System für den klinischen und administrativen Bereich im Krankenhaus. Alle relevanten Informationen und Dokumente werden digital integriert und am Arbeitsplatz zur Verfügung gestellt. DeepUnity ist ein PACS-System. Es bietet eine universelle Visualisierungslösung für medizinische Daten (DICOM und Non-DICOM) und ermöglicht den sicheren Zugriff auf alle medizinischen Daten von überall und zu jeder Zeit.

Im Jahr 2020 stand erneut eine Modernisierung der Storage-Infrastruktur des UKDD an. Neben den Daten aus HDYMedia und DeepUnity sollten zukünftig auch die Daten aus dem vom UKDD genutzten E-Mail-Management-System mit der neuen Lösung archiviert und gespeichert werden.

Wie viele IT-Verantwortliche im Gesundheitswesen sieht Gordon Schultz, Leiter der Abteilung Basisinfrastruktur der Direktion Informationstechnologie und Datenmanagement am Zentrum für Medizinische Informatik des UKDD, die Stabilität der heutigen Krankenhaus-IT vor allem durch wachsende Datenberge und damit Ransomware-Attacken und Fachkräftemangel bedroht.

Das Datenwachstum steht in engem Zusammenhang mit Kosten, Personalplanung und IT-Sicherheit, denn mehr Daten erfordern mehr Speicherplatz und neue Systeme. Diese müssen verwaltet, aktualisiert und gesichert werden. Dies wiederum erfordert IT-Spezialisten, Zeit und Geld. Mehr Systeme und Ressourcen bedeuten oft mehr Komplexität und zusätzliche Einfallstore für Cyberangriffe.

Gordon Schultz zum allgegenwärtigen Thema Bedrohung durch Ransomware:

„Eine der größten Herausforderungen, der wir uns als IT-Betrieb derzeit stellen müssen, ist die latente Gefahr von Ransomware-Angriffen. Wie können wir Patienten- und andere sensible Daten bestmöglich schützen und was passiert, wenn trotz aller Vorichtsmaßnahmen ein Cyberangriff erfolgreich war? Diese Aspekte mussten bei der Planung der Archivierungs- und Datenspeicherungssysteme unbedingt berücksichtigt werden.“

Zum Thema Auslagerung von Gesundheitsdaten in die Public Cloud teilen Gordon Schultz und sein Kollege Andreas Naumertat, Teamleiter Server/Storage/Backup, eine ähnliche Einstellung. Derzeit werden die Daten des UKDD an drei Standorten repliziert. Grundsätzlich wäre in Zukunft nach einer entsprechenden Öffnung des Sächsischen Datenschutzgesetzes für den Gesundheitsbereich die Nutzung von Cloud-Diensten für eine dieser Replikationen denkbar. Allerdings sehen sowohl Herr Schultz als

auch Herr Naumertat zunächst Daten aus Forschung und Lehre mit geringer Kritikalität als am ehesten Cloud-fähig an. Die Auslagerung von hochsensiblen Patientendaten sehen beide kritisch.

„Patientendaten, also die „Kronjuwelen“ des UKDD, ziehen wir nicht für eine Auslagerung in Betracht, solange es gute OnPrem-Alternativen gibt.“

stellt Andreas Naumertat fest.

Aufgrund der durchweg guten Erfahrungen mit der iCAS Archiv-Middleware, dem Support durch iTernity und der Empfehlung des langjährigen Partners des UKDD, der Dedalus Healthcare Group, fiel die Entscheidung schnell auf die Managed Storage-Plattform iCAS FS von iTernity.

Gordon Schultz zum Wechsel von iCAS auf iCAS FS:

„Nach den sehr guten Erfahrungen mit dem Support bei iCAS durch iTernity war es für uns leicht, uns für den durch Dedalus vorgeschlagenen Switch auf iCAS FS zu entscheiden.“

Mit iCAS FS entschieden sich die IT-Verantwortlichen des UKDD außerdem für eine Storage-Lösung, die die Vorteile der Public Cloud mit der Sicherheit von On-Premises-Lösungen verbindet – also eine Cloud Experience On-Premises.

ZIELE: CYBER- UND ZUKUNFTSSICHERHEIT, AUFWANDSREDUKTION

Folgende Ziele wollten die IT-Verantwortlichen des UKDD mit dem Wechsel von iCAS auf iCAS FS erreichen:

- Managed Storage: Administration und Monitoring sollte durch den Hersteller erfolgen, der Datenspeicher sollte kaum Aufwand für die IT-Mitarbeiter:innen des UKDD verursachen.
- Zukunfts- und Planungssicherheit: Die Lösung sollte, bei geringen Gesamtkosten, jederzeit problemlos und kurzfristig skalierbar sein, um mit den teilweise sprunghaft wachsenden Datenmengen Schritt halten zu können.
- Ransomware-Schutz: Das Risiko der unbefugten Manipulation und Löschung von Daten durch Cyberkriminelle und Mitarbeiter:innen sollte minimiert werden.
- Compliance: Alle gesetzlichen Anforderungen, z.B. aus der DSGVO (Datenschutzgrundverordnung) und dem NISG (Netz- und Informationssystemsicherheitsgesetz) mussten erfüllt sein.
- Hochverfügbarkeit: Ein unterbrechungsfreier und performanter Zugriff auf die gespeicherten Daten wurde vorausgesetzt.

ENTLASTUNG DER IT-ABTEILUNG, MEHR ZEIT FÜR KERNAUFGABEN

Managed Storage

Die Entlastung seines Teams war für Andreas Naumertat ein ganz wesentlicher Aspekt, den die neue Speicherlösung erfüllen sollte.

„Dank der Architektur von iCAS FS haben wir seit der Umstellung noch weniger Aufwand mit Archiv und Storage. Seit Abschluss der Datenmigration haben wir die Verantwortung dafür fast vollständig an iTernity abgegeben.“

stellt Andreas Naumertat fest. iTernity ist folglich für die Speicherplattform verantwortlich. Ob Implementierung, Monitoring, Fehlerbehebung, Konfigurationsänderungen oder Administration – die IT des UKDD hat kaum Berührungspunkte mit iCAS FS. Das System wird als Managed Service von iTernity betrieben und läuft reibungslos im Hintergrund.

Außerdem schätzen die Dresdner IT-Verantwortlichen, dass sie sich bei iTernity jederzeit an ihren persönlichen Ansprechpartner wenden können:

„Ein ganz wichtiger Punkt ist für uns, dass das Support-Team von iCAS FS jederzeit für uns erreichbar ist und wir persönliche Ansprechpartner haben. Auch bei technischen Herausforderungen in der Vergangenheit wurde schnell reagiert und es sind nie Daten verloren gegangen. Wir fühlen uns von iTernity in jeder Hinsicht gut betreut.“

Zukunftssicherheit

Als Scale-Out-Cluster wirkt iCAS FS dem schwer kalkulierbaren Datenwachstum entgegen. Die software-basierte Lösung lässt sich durch Hinzufügen von Cluster-Knoten einfach erweitern, denn bei dem horizontal skalierbaren System wird die Gesamtleistung von einer Vielzahl von Storage-Server-Knoten (Clustern) erbracht. Diese treten nach außen als Gesamtsystem auf und ermöglichen eine beliebige Kapazitäts- und Leistungserweiterung.

Ransomware-Schutz

Ransomware-Angriffe, Insider-Attacken, Datenverlust – viele Gefahren zwingen das UKDD aufgrund der Sensibilität der Gesundheitsdaten zu besonderen Schutzmaßnahmen. Diese sind bereits in die Architektur des Archivspeichers integriert. iCAS FS basiert auf einem gehärteten Linux-System und stellt auf Seiten des UKDD keine Administratorenzugänge zur Verfügung. Dadurch wird die Angriffsfläche für externe und interne Bedrohungen minimiert.

Dank WORM-Speicherung (Write Once Read Many) und Retention Management können Daten nach dem Schreiben nicht mehr verändert, manipuliert und gelöscht werden.

Die Aktualität des Systems wird durch den iTernity Managed Service gewährleistet, da Updates und Sicherheitspatches direkt von iTernity eingespielt werden.

Erfüllung gesetzlicher Vorgaben

Mit iCAS FS erfüllt das UKDD alle Vorgaben zur Speicherung sensibler Gesundheitsdaten. Diese Fähigkeit wurde auch durch die KPMG unabhängig geprüft und bescheinigt. Darüber hinaus liegen die Daten sicher in den eigenen Rechenzentren.

Hochverfügbarkeit

Ein unterbrechungsfreier und performanter Zugriff auf die gespeicherten Daten ist ein Muss.

Hochverfügbarkeit stellt iCAS FS dank transparentem Read/Write Failover und einem Active-Active Cluster sicher. Alle Knoten erfüllen simultan die gleichen Dienste und springen bei einem Ausfall füreinander ein.

Zusätzlich sichert das UKDD die Daten an mehreren Standorten und stellt dadurch Geo-Redundanz sowie einen Schutz vor Naturkatastrophen und Datenverlust her. iCAS FS repliziert die Daten standardmäßig synchron, kann ein einzelnes Cluster jedoch auch auf weit entfernte Rechenzentren ausweiten. In diesem Fall wechselt iCAS FS intelligent zwischen synchroner und asynchroner Replikation.

BLICK IN DIE ZUKUNFT

Neben Projekten wie der Umsetzung des KHZG und der anstehenden Integration von KI in die Medizin beschäftigt Herrn Schultz und Herrn Naumertat insbesondere die zunehmende Bedrohung durch Ransomware.

Auch das Datenwachstum, das in absehbarer Zeit z.B. durch die Digitalisierung der Pathologie befeuert wird, und damit die Planungs- und Zukunftssicherheit sind ein großes Thema. Doch für diese Herausforderung sehen sich die IT-Verantwortlichen des UKDD mit iCAS FS bestens gerüstet. Erst kürzlich stand eine Erweiterung der Speicherplattform an, die aufgrund der Skalierbarkeit jederzeit problemlos möglich ist.

Gordon Schultz schließt zufrieden ab:

„Das zukünftige Datenwachstum ist für uns sehr schwer abzuschätzen, insbesondere im Hinblick auf Forschungsdaten, Genomdaten, KI und Projekte wie z.B. die Digitalisierung der Pathologie. Hinzu kommt, dass Storage-Erweiterungen immer erhebliche Investitionen darstellen. Wir sind aber davon überzeugt, mit der kosteneffizienten und skalierbaren Plattform iCAS FS eine zukunftssichere Lösung gewählt zu haben.“

GRENZENLOSE SKALIERBARKEIT FÜR BEGRENZTE IT-BUDGETS

iCAS FS ist eine Scale-Out Speicherplattform für Archiv, Backup und geschäftskritische Daten aller Art. Die software-basierte Lösung ist ab 40 TB grenzenlos skalierbar und besticht mit geringen Gesamtkosten, einfacher Handhabung und hoher Flexibilität.



53% Kosteneinsparung im Vergleich zu Public Cloud Storage und Sie behalten dabei die Hoheit über Ihre Daten



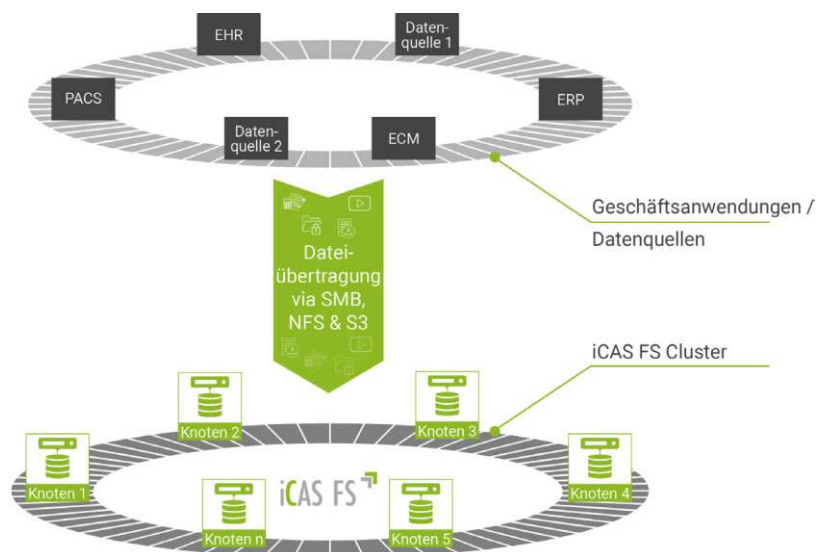
Klein starten, unbegrenzt skalieren: Scale-out ab 40 TB in einer software-basierten Speicherplattform



Die Vorteile von Public Cloud Storage im eigenen Rechenzentrum: hohe Flexibilität, einfache Skalierbarkeit, geringer Aufwand



Selbstverwaltetes System: Zero-Touch Betrieb und Managed Services mit Monitoring des gesamten Systems



iCAS FS ermöglicht zukunftsichere Datenspeicherung und Compliance bei geringen Gesamtkosten. Die Plattform eignet sich optimal für die Speicherung und den Schutz von Daten aus verschiedenen Anwendungen und Quellen und ermöglicht revisionssichere Archivierung, Ransomware-sichere Backup Speicherung sowie die Entlastung Ihrer Primärspeicher.

Die software-basierte Architektur baut auf Standardhardware und einem Linux Betriebssystem auf. Dank WORM Speicherung, S3 Object Lock, Retention Management, Verschlüsselung und Audit Trail werden Compliance und Sicherheit groß geschrieben, was auch durch die KPMG bestätigt wurde.



MÖCHTEN SIE MEHR ERFAHREN?

Vereinbaren Sie eine Demo oder diskutieren Sie Ihre Anforderungen mit uns:
info@iternity.com | +49 761 590 34 810 | www.iternity.com/demo