



Quelle: Klinikum Garmisch-Partenkirchen



Branche:
Gesundheitswesen

Land:
Deutschland

URL
<https://www.klinikum-gap.de>

Digitaler Schutzwall gegen Hacker: Klinikum Garmisch-Partenkirchen zieht die Mauer hoch

Das Krankenhaus implementiert eine hochsichere Umgebung mit Dell PowerProtect und einem isolierten Cyber Recovery Vault

Die Herausforderung

Wie viele andere Krankenhäuser auch stand das Klinikum Garmisch-Partenkirchen vor der Herausforderung, seine gewachsenen Backup-Strukturen zu modernisieren. Die vorhandene Umgebung war in die Jahre gekommen, Speicherkapazitäten stießen an ihre Grenzen und es fehlten zeitgemäße Sicherungsverfahren. Neben der reinen Erneuerung der Systeme wollte das IT-Team die Datensicherheit grundlegend erhöhen – nicht zuletzt aufgrund zunehmender Cyberbedrohungen im Gesundheitswesen. Gesucht wurde deshalb eine moderne Lösung mit einem Cyber Recovery Vault, der durch die Unveränderbarkeit der Daten höchste Resilienz sicherstellt.

Tony Liersch, Teamleiter IT-Infrastruktur & Support, Klinikum Garmisch-Partenkirchen

»Unsere Infrastruktur war sehr in die Jahre gekommen und musste aus Sicherheitsgründen komplett ausgetauscht werden. Im Rahmen der Modernisierung wollten wir die bestmögliche Lösung.«

Die Lösung

- Dell PowerProtect Data Manager als zentrale Datensicherungssoftware
- Dell PowerProtect Data Domain 6900 und 6400 als hochperformanter Backup-Speicher
- Isolierter Cyber Recovery Vault für maximale Cyberresilienz

Das Ergebnis

- Hohe Cyberresilienz durch Unveränderbarkeit der Daten
- Performantes Speichersystem durch hohe Datenreduktionsrate
- Einfaches Management dank moderner Datensicherungssoftware

Das Klinikum Garmisch-Partenkirchen ersetzt seine veraltete Bandsicherung

Das Klinikum Garmisch-Partenkirchen ist ein hochspezialisierter Anbieter anerkannter Spitzenmedizin mit überregionalem Versorgungsauftrag und zugleich fachübergreifender medizinischer Rundumversorger für die Menschen in der Region. Rund 1.500 Mitarbeitende betreuen jährlich etwa 23.000 stationäre und 45.000 ambulante Patientinnen und Patienten. Im rund 25 Kilometer entfernten Murnau betreibt das Klinikum Garmisch-Partenkirchen darüber hinaus an der renommierten Berufsgenossenschaftlichen Unfallklinik Murnau ein zusätzliches Zentrum für Innere Medizin. Hinter der medizinischen Kompetenz steht eine IT-Infrastruktur, die hochverfügbar, effizient und vor allem sicher sein muss – schließlich unterliegen Patientendaten strengen gesetzlichen Vorgaben und sind besonders schützenswert.

Die vorhandene Datensicherungsumgebung in den zwei Rechenzentren des Klinikum Garmisch-Partenkirchen genügte diesen Anforderungen jedoch nicht mehr. Die Backup-Landschaft war historisch gewachsen, basierte auf alter Bandtechnologie und einem klassischen Speichersystem. Moderne Sicherungsverfahren wie VMware-Image-Backups fehlten ebenso wie eine zweite Sicherungskopie oder ein spezieller Schutz vor Cyberangriffen. „Wir hatten eine sehr in die Jahre gekommene Infrastruktur und mussten aus Sicherheitsgründen alles austauschen“, erinnert sich Tony Liersch, Teamleiter IT-Infrastruktur & Support beim Klinikum Garmisch-Partenkirchen.

Gleichzeitig stieg der Druck auf die IT-Abteilung durch das schnelle Datenwachstum. Gesetzliche Vorgaben, der verstärkte Einsatz neuer Fachanwendungen und steigende Ressourcenanforderungen etwa durch SAP führten zu einer kontinuierlichen Zunahme des Datenvolumens. Die bestehende Infrastruktur stieß damit sowohl bei Kapazität als auch bei Ausfallsicherheit an ihre Grenzen. Für das Klinikum stand fest: Nur eine umfassende Modernisierung der Data-Protection-Umgebung kann die langfristige Sicherheit

Tony Liersch, Teamleiter IT-Infrastruktur & Support, Klinikum Garmisch-Partenkirchen

»Von Beginn an war eine gekapselte, besonders geschützte Backup-Umgebung eine zentrale Anforderung – ein sogenannter Cyber Recovery Vault, der die Sicherungskopien isoliert vorhält und sie somit selbst im Fall eines Ransomware-Angriffs unangreifbar macht.«

der Patientendaten gewährleisten und die notwendige Flexibilität für zukünftige Entwicklungen bieten.

Gesucht: Eine Lösung, die Angreifer außen vorhält

Als öffentliches Haus war das Klinikum dazu verpflichtet, die Erneuerung der Datensicherung im Rahmen einer Ausschreibung zu vergeben. Von Beginn an war eine gekapselte, besonders geschützte Backup-Umgebung eine zentrale Anforderung – ein sogenannter Cyber Recovery Vault, der die Sicherungskopien isoliert vorhält und sie somit selbst im Fall einer Ransomware-Attacke unangreifbar macht. „Es gibt ein paar IT-Hersteller, die entsprechende Lösungen anbieten. Aber keine davon ist so ausgeklügelt wie die von Dell Technologies“, erklärt Liersch.

Neben den technischen Aspekten spielten auch die Referenzen und die Kompetenz des künftigen Implementierungspartners eine entscheidende Rolle. Das Klinikum suchte nach einem Partner, der nicht nur die Technologie beherrscht, sondern auch über nachweisliche Erfahrung in der Umsetzung solcher Projekte verfügt. Ausschlaggebend waren Kriterien wie die Zahl vergleichbarer Implementierungen, die technische Expertise der Ingenieure und die Qualität des Projektmanagements.

Am Ende setzte sich die mentIQ GmbH, ein Spezialist in den Bereichen intelligentes Datenmanagement, Data Protection und Cyber Recovery, in dem mehrstufigen Vergabeverfahren gegen zwei weitere Bieter durch. „Wir wollten wissen, wie oft ein Partner so etwas schon gemacht hat und wie viel Erfahrung er in diesem Bereich mitbringt“, betont Liersch. „mentIQ hat uns hier schnell überzeugt.“

Hand in Hand entsteht ein neuer Schutzwall

Nach der Vergabe begann ein rund neunmonatiges Modernisierungsprojekt, das mentIQ in enger Abstimmung mit Dell Technologies umgesetzte. Wöchentliche Jour-fixe-Termine sorgten für eine präzise Planung und eine enge Abstimmung mit dem internen IT-Team. Die Klinik-IT war von Beginn an in die Umsetzung eingebunden, nicht nur um die bestehende Infrastruktur und die notwendigen Netzwerkinformationen bereitzustellen, sondern auch, um die neue Umgebung kennenzulernen und sie künftig eigenständig betreiben zu können.

„mentIQ hat die richtigen Strategien und zeichnet sich durch ein hervorragendes Projektmanagement aus. Das heißt, wir konnten uns mehr oder weniger entspannt zurücklehnen“, sagt Liersch rückblickend. Dell Technologies begleitete den Partner im Hintergrund und stand für technische Rückfragen bereit. Das Zusammenspiel zwischen Klinikum, mentIQ und Dell Technologies verlief reibungslos und legte den Grundstein für eine zukunftssichere Backup-Strategie.

Tony Liersch, Teamleiter IT-Infrastruktur & Support, Klinikum Garmisch-Partenkirchen

»Die hohen Anforderungen, die wir hatten, konnte nur die Lösung von Dell Technologies erfüllen. Der Partner mentIQ – und damit die Experten von Dell Technologies im Hintergrund – hat uns perfekt durch das Projekt begleitet.«

Digitaler Tresor liefert einmalige Sicherheit

Mit der Einführung von Dell PowerProtect hat das Klinikum Garmisch-Partenkirchen seine Datensicherung auf ein neues Niveau gehoben. Anstelle veralteter Bänder sorgt nun eine moderne, softwaregesteuerte Backup-Umgebung für die Sicherung der Daten in den beiden Rechenzentren des Klinikums. Die Kombination aus Dell PowerProtect Data Manager und den skalierbaren PowerProtect Data Domain Appliances bietet nicht nur eine hohe Datenreduktionsrate und damit schnelle Backup-Zeiten, sondern auch ein einfaches, zentrales Management der gesamten Umgebung.

Eine Kernkomponente ist der isolierte Cyber Recovery Vault. Er stellt sicher, dass eine Kopie der kritischen Patientendaten in einer abgeschotteten Umgebung vorgehalten wird, die selbst im Fall eines erfolgreichen Cyberangriffs nicht kompromittiert werden kann. Damit hat das Klinikum eine entscheidende Maßnahme zur Stärkung seiner Cyberresilienz umgesetzt – ein Aspekt, der angesichts steigender Ransomware-Angriffe im Gesundheitswesen von existenzieller Bedeutung ist.

Auch die Skalierbarkeit der neuen Umgebung erweist sich als wichtiger Vorteil. Die IT-Abteilung kann flexibel auf künftiges Datenwachstum reagieren, das beispielsweise durch neue klinische Anwendungen oder erweiterte SAP-Anforderungen entsteht. „Unsere Umgebung verändert sich extrem schnell“, so Liersch. „mentIQ und Dell haben darauf hervorragend reagiert.“ Zum Zeitpunkt der Inbetriebnahme lag die Auslastung der Systeme bei rund 70 Prozent, sodass ein komfortabler Puffer für weiteres Wachstum vorhanden ist.

Ein internes Audit, das von Fachkollegen der Sana Kliniken durchgeführt wurde, würdigte die Qualität der Umsetzung ausdrücklich und bestätigte die Leistungsfähigkeit der neuen Lösung. Für das IT-Team bedeutet die Modernisierung nicht nur mehr Sicherheit, sondern auch deutlich weniger Aufwand im laufenden Betrieb. Die Administration der Datensicherung ist einfacher und übersichtlicher geworden, sodass sich die Mitarbeitenden stärker auf strategische Aufgaben konzentrieren können.

Diese Success Story entstand in enger Zusammenarbeit mit Dell Technologies.

mentIQ GmbH

Seit 2007 konzipiert, realisiert und unterstützt mentIQ intelligente Lösungen für effizientes und zukunftsweisendes Daten- und Informationsmanagement. Das Portfolio erstreckt sich von der Beratung der Kunden zu künftigen Datenmanagement Strategien über den Vertrieb und die Realisierung entsprechender Lösungen für das Speichern, Sichern und Aufbewahren von Daten bis hin zu Services, die es ermöglichen, maximale Mehrwerte aus diesen Lösungen zu ziehen. Proaktiver Support und Fehlervermeidung statt Fehlerbehebung stehen im Kern dieser maßgeschneiderten Services. Dabei unterstützt uns unsere eigens entwickelte Service Plattform ONEIn-sight mit Asset Management, Monitoring und Auto-Support.

Kontakt
mentIQ GmbH
Otto-Hahn-Straße 20
85609 Dornach

Tel.: 089 - 95 415 72 - 20
info@mentiq.com