Außenansicht des Klinikums Rosenheim

Hochverfügbare Sicherheitslösung im Klinikum Rosenheim

Notfallserver im Dienste der Gesundheit

Wenn der Chirurg nicht auf die Patientendaten zugreifen kann oder in der Radiologie die digitalen Röntgenbilder vor einer Operation nicht verfügbar sind, kann das im schlimmsten Fall Leben kosten. Daher sichert das Klinikum Rosenheim einen Teil seiner Server-Infrastruktur mit einem neuen Notfallserver ab. Im Juli 2008 konnte die Lösung ihre Qualität beweisen.

Das Klinikum im oberbayerischen Rosenheim ist als Schwerpunktkrankenhaus der Versorgungsstufe II und Lehrkrankenhaus der Ludwig-Maximilians-Universität München mit zwölf Fachabteilungen (einschließlich Belegabteilung), knapp 200 Ärzten, 429 Schwestern und Pflegern sowie einer Verwaltung mit rund 100 Mitarbeitern eine große Einrichtung seiner Art. Entsprechend der modernen Ausstattung ist der IT-Durchdringungsgrad bei hundert Prozent: „Wenn bei uns bestimmte Systeme ausfallen, ist die ganze Klinik paralysiert. Vor allem die Umstellung der Radiologie auf digitale Röntgenbilder und ein entsprechendes Bildarchiv erforderten eine zuverlässige Notfallabsicherung", erläutert Helmut Weis, Leiter der IT-Abteilung im Klinikum Rosenheim.

Hohe Sicherheitsanforderungen

Entsprechend diesen Anforderungen wurde zunächst eine Cluster-Lösung für die wichtigsten Server in Betracht gezogen. „Die ersten Erfahrungen damit waren allerdings nicht sehr erfreulich", erklärt Weis. „Der Cluster bestand aus zwei identischen Servern, die permanent miteinander abgeglichen werden mussten. Dabei war darauf zu achten, dass keine Fehler gespiegelt wurden. Die Administration und die regelmäßigen Tests waren sehr zeitaufwändig, zudem war die Cluster-Lösung – im Endausbau – mit rund 100.000 Euro teuer, weil wir Betriebssysteme und Datenbanken doppelt vorhalten mussten", so Weis weiter.

Hochverfügbarkeit bei niedrigeren Kosten

Daher beschlossen die IT-Spezialisten des Klinikums, nach einer anderen Lösung zu suchen. Ziel war die Systemwiederherstellung nach maximal 30 Minuten und ein Datenverlust von höchstens vier Stunden. Fündig wurde man bei dem IT-Dienstleister ACP IT Solutions AG, mit dem das Klinikum bereits erfolgreich zusammenarbeitete. Im April 2006 stellte ACP den von der Firma Nets GmbH entwickelten Notfallserver vor, den das Unternehmen unter seinem Markennamen „Rescudo" anbietet. Dabei handelt es sich um eine durchgängige und transparente, hardware- und applikationsunabhängige Lösung, mit der beliebig viele Windows-Server abgesichert werden können.

Was wurde wie abgesichert?

Im Klinikum Rosenheim sollten folgende Server in das Sicherheitskonzept integriert werden:

1. File-Server, gleichzeitig auch Anmeldeserver im Active Directory (AD)
2. Exchange-Server mit zweitem Anmeldeserver für AD
3. OrgaCard-Server für Speiseversorgung
4. PACS-Server (Picture Archiving Communication System) für alle Röntgenbilder mit 1,7 TB Speichervolumen
5. Server für die Chargendokumentation für die Sterilisationssysteme
6. Server für die geburtshilfliche Kreißsaaldokumentation

„Als neue Hardware, auf dem die Notfallserver-Software installiert werden sollte, schafften wir einen neuen Windows-Server 2003 mit zwei CPU à drei GHz und 4,2 Terabyte Plattenspeicher an, der in einem abgesicherten separaten Brandabschnitt aufgebaut wurde", so der IT-Leiter der Klinik.

Plug & Play Protection

Das Sicherheitsprojekt wurde durch Robert Pfaffinger von der ACP IT Solutions AG in Zusammenarbeit mit zwei IT-Spezialisten der Klinik durchgeführt. Im ersten Schritt installierte der Techniker die Notfallserver-Software auf dem neuen Windows-Rechner. Der nächste Schritt umfasste die Replikation aller abzusichernden Primärsysteme auf dem Notfallserver. Dabei erzeugte der Notfallserver von jedem Produktivsystem ein Abbild in seinem Imagepool. Die Dateien dieser 1:1-Kopien wurden mit den Attributen und Zugriffsrechten aller Mitarbeiter gesichert. Die systemkritische Komponente „Active Directory" wird über spezielle Microsoft-Systemfunktionen gesichert, um die Startfähigkeit der Abbilder auch in kritischen Situationen – zum Beispiel beim Ausfall eines Servers während der Replikation – zu garantieren.

Helmut Weis, Leiter der IT-Abteilung im Klinikum Rosenheim: Ziel war die Systemwiederherstellung nach maximal 30 Minuten und ein Datenverlust von höchstens vier Stunden.

Nachdem die erste Replikation abgeschlossen war, erfolgen in frei definierbaren Zeitabständen alle weiteren Kopiervorgänge inkrementell auf 64k-Blockebene: Das bedeutet, es werden Zug um Zug nur die Dateien gesichert, die tatsächlich neu hinzugekommen sind. Dieses Volumen-sparende Vorgehen belastet das Klinik-Netz kaum.

„Eine etwas knifflige Aufgabe war allerdings die Justierung des regelmäßigen Datenabgleichs zwischen den Servern, weil hier so unterschiedliche Größenordnungen anfallen. So kann der Server für die Chargendokumentation der Sterilisationsprozesse halbstündlich repliziert werden, weil lediglich wenige Daten anfallen. Das Archiv für Röntgenbilder dagegen erlaubt nur dreimal täglich eine Aktualisierung auf dem Notfallserver, weil 1,7 Millionen Files im Umfang von rund zwei Terabyte Daten abzugleichen sind", schildert Weis. „Um hier ein optimales Prozedere zu etablieren, mussten anfangs einige Tests durchgeführt werden. Heute werden die Daten der sechs Server jeweils angepasst an die Notwendigkeit und Möglichkeit auf dem Notfallserver aktualisiert, um im Falle eines Crashs möglichst geringe Datenverluste in Kauf nehmen zu müssen – von einstündigen bis zu dreimal täglichen Rhythmen. In der Nacht läuft eine ‚Equal-Funktion', in der das System überprüft, ob auch wirklich alle Daten gleich sind. So müssen zum Beispiel auf dem Primärsystem gelöschte Dateien auch auf dem Notfallserver gelöscht werden", so Weis weiter. Insgesamt dauerte das Projekt – von der Anschaffung des Notfallservers bis zur fertigen Replikation aller Primärsysteme und notwendigen Tests – etwa sechs Wochen.

Backup-System in zehn Minuten als vollwertiger File-Server

Was bisher nur theoretisch getestet wurde, musste sich Anfang Juli 2008 zum ersten Mal auch in der Praxis beweisen: Nachdem ein Hardwarefehler des zentralen File-Servers zu einem kompletten Ausfall des RAID-Systems geführt hatte und eine Wiederherstellung kurzfristig nicht möglich war, schlug die Stunde des Notfallservers. Während in Stresssituationen dieser Art meistens Hektik ausbricht, blieb man in der IT-Abteilung gelassen, weil sich das Backup-System schnell per Mausklick aktivieren ließ und innerhalb von zehn Minuten als vollwertiger File-Server zur Verfügung stand. Angenehm für die Administration ist, dass sich mit Hilfe des Notfallservers alle Schritte vom Ausfall des Primärsystems bis zu seiner Wiederinbetriebnahme komfortabel über eine grafische Oberfläche steuern lassen. Nachdem das Backupsystem als „neuer" File-Server lief, war für die User keinerlei Unterschied zwischen dem normalen und dem Ausfallserver zu spüren. Der Datenverlust betrug rund vier Stunden, wobei allerdings nur zwei Stunden der normalen Arbeitszeit betroffen waren. Da es drei Tage dauerte, das RAID-System wieder herzustellen, ersetzte der Notfallserver das Primärsystem in dieser Zeit problemlos.

Wiederherstellung ohne Ausfallzeit

Sobald der ursprüngliche File-Server wieder verfügbar war, mussten die Daten vom laufenden Notfallsystem auf das Primärsystem überspielt werden. Dieser Wiederherstellungsprozess entsprach im Grunde der umgekehrten Replikation und wurde über Nacht in zwei Schritten durchgeführt: Noch während des Notbetriebs replizierte der Administrator das weiterhin auf dem Notfallserver laufende Produktivsystem auf die reparierte Hardware. Anschließend schaltete er den Notfallserver wieder zurück in seine eigentliche Funktion und kopierte die in der Übergangszeit neu hinzugekommenen Daten inkrementell nochmals auf das wieder hergestellte Produktivsystem. „Die Inbetriebnahme des Originalsystems erfolgte ohne spürbare Ausfallzeit", erläutert Helmut Weis.

Der Ausfall des RAID-Systems bewies, dass die Anschaffung des Notfallservers die richtige Strategie war. Auch mit den Kosten von 30.000 Euro hielt sich die hochverfügbare Sicherheitslösung für das Klinikum Rosenheim in einem realisierbaren Rahmen.