VARONIS CASE STUDY

Universitätsklinikum Freiburg

„Um Daten intern, aber auch mit externen Partnern sicher auszutauschen, haben wir verschlüsselte E-Mails und Festplatten verwendet. Bei etwa 10.000 Mitarbeitern sind wir mit dieser Methode schließlich an unsere Grenzen gestoßen. Mit DatAnywhere haben wir jetzt eine Filesharing-Lösung, die unseren Datenschutzstandards entspricht und die sich in die bestehende Infrastruktur integrieren lässt. Mit den bestehenden Berechtigungskonzepten und ohne redundante Datenhaltung.“

—Thorsten Dres
DV-Systemtechniker im Klinikrechenzentrum des Universitätsklinikums Freiburg

DER KUNDE

UNIVERSITÄTSKLINIKUM FREIBURG

ORT

Freiburg im Breisgau, Deutschland

BRANCHE

Gesundheitswesen, Universitätsklinikum mit Forschung, Lehre und Krankenversorgung

PRODUKT

Varonis DatAnywhere

Das Universitätsklinikum Freiburg gehört mit etwa 10.500 Mitarbeiterinnen und Mitarbeitern zu den größten Universitätskliniken in Deutschland. Rund 1.400 Ärztinnen und Ärzte sowie mehr als 2.900 Pflegekräfte versorgen pro Jahr 64.000 Patientinnen und Patienten stationär sowie rund 580.000 Fälle ambulant. Damit ist das Universitätsklinikum der größte Arbeitgeber Südbadens. Es verbindet in seiner originären Aufgabe Forschung, Lehre und Krankenversorgung stets mit dem Ziel, den Patienten eine an den neuesten Erkenntnissen der Wissenschaft ausgerichtete Behandlung zu bieten. Im Klinikum arbeiten alle Berufsgruppen in einem multiprofessionellen Team zusammen und tauschen sich kontinuierlich aus. Mit seinen internen und externen Partnern im Gesundheitswesen steht das Uniklinikum Freiburg in einem konstruktiven Dialog.

BUSINESS BENEFITS

SICHERER DATENAUSTAUSCH MIT EXTERNEN KOOPERATIONSPARTNERN OHNE DOPPELTE DATENHALTUNG

In der Forschung entstehen heutzutage sehr große Datenmengen, welche mit unterschiedlichen Kooperationspartnern weltweit ausgetauscht werden müssen. Um große Datenmengen sicher austauschen sowie eine Kontrolle und die Protokollierung sicherzustellen, wird hier DatAnywhere verwendet. Durch DatAnywhere haben Forscher im Universitätsklinikum Freiburg die Möglichkeit, gezielt bestimmte Dateien oder ganze Verzeichnisse sicher mit Externen zu teilen. Sowohl ein externer Upload als auch ein Download ist möglich. Zusätzlich findet eine Kontrolle statt, da jeder Download und Upload eines externen Kooperationspartnern protokolliert und dem/der Klinikums Mitarbeiter/in mitgeteilt wird. So kann dem/der Klinikums Mitarbeiter/in jederzeit nachvollziehen, ob ein bestimmter Partner ein Dokument bereits heruntergeladen hat.

INTEGRATION IN BESTEHENDE SYSTEME – OPTIMALE SYNCHRONISATION MIT MOBILEN ENDGERÄTEN

Innerhalb des Universitätsklinikums Freiburg greifen etwa 10.000 Benutzer auf die Windows-Fileserver und einen Datenbestand von 82 Terabyte zu. Dieser Datenbestand umfasst im Wesentlichen allgemeine Unternehmensdaten. Die Patientendaten werden in einem eigenen KIS (Klinikinformationssystem) gespeichert und verwaltet. Für jeden Bereich gibt es einen oder mehrere eigene IT-Verantwortliche, die für die Benutzer vor Ort den First-Level Support übernehmen und innerhalb Ihres Bereiches für die gesamte IT verantwortlich sind. Unter anderem regeln sie auch die Berechtigungen. Die dezentral gesteuerten Berechtigungen von AD-Verzeichnissen werden im Rechenzentrum wiederum über ein zentrales webbasiertes System (Eigenentwicklung) realisiert. Die DatAnywhere-API lässt sich mittels Webservices ansteuern und so in das bestehende System integrieren.

ENTSPRICHT DEN HOHEN DATENSCHUTZSTANDARDS IM GESUNDHEITSWESEN

Die Lösung wird den hohen Datenschutzstandards gerecht und lässt sich gleichzeitig in die vorhandene Infrastruktur integrieren. Es sollte auf jeden Fall gewährleistet sein, dass die Daten mit externen Mitarbeitern und Partnern ausgetauscht werden können und der Zugriff über mobile Endgeräte abgesichert ist. Die bestehenden Berechtigungskonzepte sollten dabei nicht aufgebrochen werden. Der Hauptvorteil kristallisierte sich schnell heraus, nämlich die Daten sicher und problemlos auch mit einer Vielzahl von externen Partner aus dem Gesundheitswesen austauschen zu können.

DIE HERAUSFORDERUNGEN

SICHERER DATENAUSTAUSCH INTERN UND MIT EXTERNEN PARTNERN

Thorsten Dres, DV-Systemtechniker im Klinikrechenzentrum des Universitätsklinikums Freiburg: *„Um die Daten intern, aber auch mit externen Partnern sicher auszutauschen, haben wir verschlüsselte E-Mails und Festplatten verwendet. Bei etwa 10.000 Mitarbeitern sind wir mit dieser Methode schließlich an unsere Grenzen gestoßen.“*

UNTERSCHIEDLICHE BEREICHE MIT UNTERSCHIEDLICHEN ANFORDERUNGSPROFILEN

Insbesondere Forschung und Lehre stellen hohe Anforderungen an digitale Informationssysteme, vor allem, wenn es darum geht, diese Daten auch untereinander auszutauschen und gemeinsam daran zu arbeiten. Sich über den aktuellen Stand der Ergebnisse auf dem Laufenden zu halten, aber auch externe Kooperationspartner zu informieren, ist unabdingbar. In den Forschungsabteilungen ist es zudem wichtig, flexibel und unabhängig von Uhrzeit und Ort auf Ergebnisse zugreifen zu können, statt in der Klinik auf Resultate zu warten. Um die verschiedenen Klinikbereiche und Abteilungen zu koordinieren, müssen die entsprechend autorisierten Benutzer Daten untereinander und gegebenenfalls mit externen Partnern austauschen sowie mit den zahlreich eingesetzten mobilen Endgeräten. Ein Beispiel aus der Lehre: In der Klinik für Zahnärztliche Prothetik wird momentan jedem Student in den ersten beiden Semestern ein eigenes iPad ausgeliehen. Durch DatAnywhere können die Studenten mobil auf Studienunterlagen zugreifen und sich zusätzlich in einem geeigneten virtuellen Raum darüber austauschen. So bleiben alle Unterlagen innerhalb der eigenen Server und werden nicht auf fremden Servern gespeichert.

EINE LÖSUNG FINDEN, DIE DEN HOHEN DATENSCHUTZSTANDARDS IM GESUNDHEITSWESEN ENTSPRICHT

Thorsten Dres: *„Wir suchten nach einer Cloud-Lösung, die unserem hohen Datenschutzstandard gerecht wird und die sich gleichzeitig in unsere vorhandene Infrastruktur integriert.“* Es sollte auf jeden Fall gewährleistet sein, dass wir Daten mit externen Mitarbeitern und Partnern austauschen können und der Zugriff über mobile Endgeräte abgesichert ist.

KEINE DOPPELTE DATENHALTUNG, BESTEHENDE BERECHTIGUNGSKONZEPTE BEIBEHALTEN

Wir hatten allerdings zwei Bedingungen: *„Wir wollten keine redundante Datenhaltung verursachen und vor allem die bestehenden Berechtigungskonzepte nicht aufbrechen“.*

ENTSCHEIDUNGSFINDUNG UND EVALUIERUNG– PASSGENAUE LÖSUNG

Im Rahmen dieses Anforderungsprofils folgte eine ausführliche Recherchephase in der insgesamt acht verschiedene Lösungen unter die Lupe genommen wurden. Drei davon kamen neben DatAnywhere von Varonis in die engere Auswahl. „Wir sind über eine simple Internetrecherche auf die Lösung gestoßen und haben sie zunächst drei Monate lang ausführlich getestet. Der Hauptvorteil kristallisierte sich schnell heraus, nämlich die Daten sicher und problemlos auch mit einer Vielzahl von externen Partner aus dem Gesundheitswesen austauschen zu können.“ Nach der erfolgreich abgeschlossenen Testphase ging die Lösung in eine insgesamt 13-monatige Pilotierung, die im September 2014 abgeschlossen worden ist.

DIE LÖSUNG

DatAnywhere erweitert die Funktionalität der unternehmensinternen Filesharing-Infrastruktur, sodass traditionelle Dateiserver als Cloud-Dienste, ähnlich wie Dropbox, verwendet werden können. Das ist über unterschiedliche Plattformen wie Windows, Mac OS X, iOS , Android und Windows Phone möglich. Cloud-Computing und ein steigendes Angebot an kostenlosen Software-Tools zum Austausch von Daten haben die Arbeitsweise und die Art, wie Informationen zwischen einzelnen Mitarbeitern, Projektgruppen und Teams ausgetauscht werden im Gesundheitswesen drastisch verändert. Zudem benötigen immer mehr Mitarbeiter mobilen Zugriff auf Systeme, ohne dass die IT bei der Sicherheit Kompromisse eingehen oder sich mit verwaltungsaufwändigen Tools herumschlagen will.

AUSTAUSCH MIT EXTERNEN KOOPERATIONSPARTNERN

In der Forschung entstehen heutzutage sehr große Datenmengen, welche mit unterschiedlichen Kooperationspartnern weltweit ausgetauscht werden müssen. Um sicher große Datenmengen auszutauschen und Kontrolle sowie Protokollierung sicherzustellen, wird hier DatAnywhere verwendet. Durch DatAnywhere haben Forscher im Universitätsklinikum Freiburg die Möglichkeit gezielt bestimmte Dateien oder ganze Verzeichnisse sicher mit externen zu teilen. Sowohl ein externer Upload wie auch ein Download ist möglich.

Ein/e Klinikums Mitarbeiter/in sendet an eine oder mehrere E-Mail-Adressen einen mit einer PIN verschlüsselten Link. Nur der Empfänger des Links kann ihn öffnen, da bei jedem Aufruf des Links eine neue PIN generiert und an die Empfänger-E-Mail-Adresse gesendet wird. Zusätzlich ist der Link mit einem Verfallsdatum versehen. Ist das Verfallsdatum erreicht, ist der Zugriff nicht mehr möglich. Dem/der Klinikums Mitarbeiter/in ist es jederzeit möglich den Zugriff sofort zu beenden. Im Hintergrund werden alle auf diese Weise erstellten Links protokolliert. Wer hat zu welchem Zeitpunkt, an welche Partner, welche Dokumente freigegeben? Zusätzlich findet eine Kontrolle statt, da jeder Download und Upload eines externen Kooperationspartners protokolliert und dem/der Klinikums Mitarbeiter/in mitgeteilt wird. So kann der/die Klinikums Mitarbeiter/in jederzeit nachvollziehen, ob ein bestimmter Partner ein Dokument bereits heruntergeladen hat.

ORGANISATIONSTRUKTUR UND INTEGRATION IN BESTEHENDE SYSTEME – MOBILER ZUGRIFF

Tools wie DatAnywhere stellen die Funktionalität von Cloud-Diensten auf der vorhandenen Infrastruktur zur Verfügung. Das umfasst die Dateisynchronisation mit vorhandenen CIFS-Shares über HTTPS sowie den Zugriff über Mobilgeräte. Bestehende Directory Services und CIFS-Berechtigungen, die Anwendung von Synchronisationslisten, verschiedene Geräteprofile und eine dezentrale Skalierbarkeit bleiben erhalten.

Innerhalb des Universitätsklinikums Freiburg greifen etwa 10.000 Benutzer auf die Windows-Fileserver und einen Datenbestand von 82 Terabyte zu. Dieser Datenbestand umfasst im Wesentlichen allgemeine Unternehmensdaten. Die Patientendaten werden in einem eigenen KIS (Klinikinformationssystem) gespeichert und verwaltet. Für jeden Bereich gibt es einen oder mehrere eigene IT-Verantwortliche, die für die Benutzer vor Ort den First-Level Support übernehmen und innerhalb Ihres Bereiches für die gesamte IT verantwortlich sind. Unter anderem regeln sie auch die Berechtigungen. Die dezentral gesteuerten Berechtigungen von AD-Verzeichnissen werden im Rechenzentrum wiederum über ein zentrales webbasiertes System (eine Eigenentwicklung) realisiert.

Die DatAnywhere-API lässt sich mittels Webservices ansteuern und so in das bestehende System integrieren. Wenn nun ein neues oder bestehendes Verzeichnis innerhalb der Cloud verfügbar gemacht oder geändert werden soll, kann dies der IT-Verantwortliche für seinen Bereich über das interne System aktivieren. Im Hintergrund wird dann die DN-API angesprochen.

IM DETAIL

Das Verzeichnis wird in DatAnywhere als Root Folder hinzufügt. Anschließend wird überprüft, ob ein Arbeitsbereich für diesen Bereich existiert, ist keiner vorhanden wird ein neuer erstellt. Der vorhandene beziehungsweise neu erstellte Arbeitsbereich bekommt dann eine neue Regel, die den Zugriff steuert. Diese Regel enthält die passenden Ressourcen AD-Gruppen für Lese- und Schreibrecht. Existieren mehrere Verzeichnisse innerhalb eines Arbeitsbereiches so existieren auch gleich viele Regeln, die mit ODER'-Verbindung verknüpft werden. Zusätzlich wird ein Auto Subscribe eingerichtet. Sämtliche Prozesse werden über PowerShell-Befehle durch das interne Administrationssystem geprüft und über einen Webservice der DatAnywhere-API weitergegeben.

DAS RESULTAT

Der Anwender sieht auf allen Endgeräten (Webinterface, Windows, MAC, Android, Windows Phone, iOS) den Arbeitsraum seines Bereichs beziehungsweise seiner Bereiche nur, wenn dort ein Verzeichnis enthalten ist, auf den dieser Anwender zugreifen kann. Zusätzlich eingerichtete Home Container sorgen dafür, dass jedes Home-Verzeichnis dem Anwender automatisch zur Verfügung gestellt wird. Alle Endgeräte, die einen Zugriff erhalten, sind zentral vom Klinikrechenzentrum gemanagte Geräte. So ist bei Laptops zusätzlich zu den auf den Geräten verteilten Richtlinien auch eine Festplattenverschlüsselung (Bitlocker, FileVault) Pflicht, um den Cloud Service nutzen zu können. Die mobilen Geräte werden durch ein MDM-System mit Richtlinien versorgt. Unter anderem einer Passwortrichtlinie, die zum Beispiel bei einem iPad vorschreibt, dass eine achtstellige Passwortkombination mit Zahlen, Buchstaben und mindestens zwei Sonderzeichen auf dem Gerät gesetzt werden soll. Zusätzlich wird nach der fünften Falscheingabe des Passworts das gesamte Gerät gelöscht. Eine zentrale Löschung und Ortung ist jederzeit über das MDM gewährleistet.

PERSPEKTIVE

Die Gerätefreigaben sollen über die DN-API realisiert werden. Windows-Laptops werden dann automatisch freigegeben, wenn sie in der Uniklinik-Domäne liegen und eine Bitlocker-Verschlüsselung aktiviert haben. Mobile Geräte (Android, iOS, Windows Phone) sollen zukünftig mit dem vorhandenen MDM-System abgeglichen sowie eine zertifikatsbasierte Anmeldung auf allen Endgeräten eingerichtet werden.

FAZIT

Thorsten Dres abschließend: *„Mit DatAnywhere haben wir jetzt eine Filesharing-Lösung, die unseren Datenschutzstandards entspricht und die sich in die bestehende Infrastruktur integrieren lässt.“*

ÜBER VARONIS

Varonis ist ein führender Anbieter von Software-Lösungen für unstrukturierte, manuell generierte Unternehmensdaten. Varonis bietet eine innovative Software-Plattform, mit der Unternehmen ihre unstrukturierten Daten abbilden, analysieren, verwalten und migrieren können. Varonis spezialisiert sich auf manuell generierte Daten, eine Art der unstrukturierten Daten, die Unternehmensdaten, wie Tabellen, Textverarbeitungsdokumente, Präsentationen, Audio–und Videodateien, E-Mails, Textmitteilungen und andere durch Mitarbeiter generierte Daten umfasst.

Derartige Daten enthalten häufig betriebliche Finanzinformationen, Produktpläne, strategische Initiativen, geistiges Eigentum und verschiedene andere wichtige Informationsformen. IT–und Business–Personal nutzen die Varonis-Software für verschiedenste Anwendungsfälle, einschließlich Data Governance, Datenschutz, Archivierung, Dateisynchronisation, verbesserter mobiler Datenverfügbarkeit und Informationsaustausch.

KOSTENLOS TESTEN:

Erfahren Sie mehr über Varonis DatAnywhere und registrieren Sie sich für einen kostenlosen Download (für maximal 5 Nutzer).

KOSTENLOSEN TEST JETZT STARTEN