

HOCH automatisiert seine Rollenvergabe mit OpenText IGA

Weniger Sonderlogik, mehr Automatisierung: Das größte Gesundheitsunternehmen der Ostschweiz löst seine gewachsene IAM-Lösung ab und vergibt Rollen und Rechte auf Basis von HR-Daten.

HOCH Health Ostschweiz hat gemeinsam mit IPG sein Identity und Access Management erneuert. Im Mittelpunkt standen die Automatisierung der Rollen- und Rechtevergabe, ein standardisiertes Datenmodell und eine wartbare technische Basis. Eine besondere Aufgabe war die Konsolidierung und Migration von rund 2,5 Millionen Rollenzuweisungen. Heute steuern HR-Informationen einen großen Teil der Berechtigungsvergabe automatisch. Erfahren Sie, wie HOCH und IPG die gewachsene Sonderlogik zurück zum Produktstandard geführt haben.





hoch Health Ostschweiz

HOCH Health Ostschweiz ist das größte Gesundheitsunternehmen der Ostschweiz und betreibt vier Standorte in St. Gallen, Grabs, Uznach und Wil. Das Kantonsspital St. Gallen ist ein universitäres Lehr- und Forschungsspital. HOCH beschäftigt mehr als 8.000 Mitarbeitende und erzielt einen Umsatz von rund 1,4 Milliarden Schweizer Franken. Pro Jahr werden rund 63.000 Patient:innen stationär und etwa 890.000 ambulant behandelt.

Before the Shift

IAM-Lösung war über ihren ursprünglichen Zweck hinausgewachsen

Ein IAM-System bleibt selten bei seinem ursprünglichen Zweck: Über die Jahre kommen neue Aufgaben, Prozesse und Systeme hinzu. So auch bei HOCH. Dort war seit 2012 eine Lösung auf Basis der Omada Identity Suite im Einsatz, ursprünglich beschafft für das Management des Active Directory. Aus der zunächst begrenzten Anwendung entwickelte sich eine umfassende IAM-Lösung.

Mit dem Ausbau wuchs die individuelle Logik. Anforderungen der Spitalregionen, insbesondere Mehrfachanstellungen innerhalb eines Instituts, führten zu einem Datenmodell, das vom Produktstandard abwich. Zahlreiche Funktionen und Prozesse entstanden als Custom Code. Das beeinträchtigte Release-Fähigkeit, Performance, Stabilität und Wartbarkeit.

Für die Erneuerung, bei HOCH als Projekt IAM2 geführt, definierte das Departement IT klare Ziele:

- die bestehende Lösung bei erhaltenem Funktionsumfang ablösen
- Rollen und Rechte auf Basis von HR-Informationen weitgehend automatisch vergeben
- manuelle Rollenansprüche und Mutationen in Fachbereichen und Kliniken reduzieren
- Standardfunktionen nutzen, um Release-Fähigkeit und Wartbarkeit zu sichern
- Usability und Self Service verbessern
- die Migration für Endanwender:innen störungsarm gestalten

Warum IPG?

HOCH wählte IPG im Rahmen einer Ausschreibung aus. IPG hatte das beste Gesamtangebot eingereicht und in der Evaluation die meisten Punkte erreicht. Hinzu kamen die Erfahrung und der Track Record aus IAM-Umsetzungsprojekten.

Die Aufgabe ging über die technische Einführung einer neuen Plattform hinaus. Datenmodelle, Rollenlogik und bestehende Prozesse mussten geprüft und für die neue Lösung neu abgebildet werden. Gerade bei gewachsenen IAM-Strukturen war relevant, welche Logik weiterhin benötigt wurde und welche Anforderungen sich mit Funktionen des Produkts lösen ließen.

The Shift

Zurück zum Standard mit OpenText IGA

Die Hauptphase bis zum Rollout des Projekts lief über zwei Jahre. Als neue technologische Basis wählte HOCH OpenText Identity Manager und OpenText Identity Governance.

Im neuen Modell ist die Rollen- und Rechtevergabe eng an das HR-System gekoppelt. Aus den dort gepflegten Attributen leitet die Lösung ab, welche Berechtigungen Beschäftigte aufgrund ihrer Funktion benötigen. Das funktioniert für interne wie für externe Accounts.

Die IAM-Plattform stellt die Berechtigungen anschließend für angebundene Systeme bereit, darunter Active Directory, Exchange, SAP, Telefonie und das Klinikinformationssystem. Wo eine technische Integration nicht sinnvoll möglich ist, greifen definierte manuelle Provisioning-Prozesse.

2,5 Millionen Rollenzuweisungen kontrolliert migriert

Ein Schwerpunkt des Projekts lag auf der Migration. Rund 2,5 Millionen Rollenzuweisungen mussten aus der bisherigen IAM-Lösung konsolidiert und in die neue Umgebung übertragen werden.

Die Migration betraf dabei nicht nur technische Datensätze. Die Rollenzuweisungen bildeten gewachsene Organisationsstrukturen ab und mussten in das neue Daten- und Rollenmodell überführt werden.

Für diesen Initial Load entwickelten HOCH und IPG ein Framework auf Basis einer Datenbank und Python-Skripten. Damit ließ sich die Migration mehrfach unter vergleichbaren Bedingungen durchführen. Soll-Ist-Vergleiche machten Abweichungen im laufenden Betrieb sichtbar und sicherten die Qualität vor der endgültigen Übernahme.

Bei IAM-Projekten müssen die Prozesse End-to-End gedacht werden. Eine enge Kopplung mit dem HR-System, gut modellierte Business-Rollen und ein hoher Automatisierungsgrad sind aus unserer Sicht wesentliche Voraussetzungen. IPG hat uns bei dieser Neuordnung von der Evaluation bis zum Rollout begleitet.

Michael Stahlberger

Leiter Departement IT und Mitglied
der Geschäftsleitung
HOCH Health Ostschweiz



After the Shift

HR-Daten übernehmen mehr Arbeit in der Rollenvergabe

Mit der neuen Lösung verwaltet HOCH Rollen und Berechtigungen auf einer vereinheitlichten Grundlage. Der Nutzen zeigt sich vor allem im täglichen Betrieb. Für HOCH bedeutet das:

- Weniger manuelle Schritte: HR-Attribute steuern einen größeren Teil der rollenbasierten Vergabe automatisch. Fachbereiche und Kliniken benötigen weniger Rollenanträge und Mutationen.
- Einheitliche Prozesse: Die IAM-Prozesse laufen über die verschiedenen Spezialistenteams hinweg nach denselben Regeln.
- Standardisierte Datenmodelle: Mehrfachanstellungen sind im Produktstandard abgebildet statt in Sonderlogik.
- Bessere Wartbarkeit: Weniger Custom Code erleichtert Wartung und Versionswechsel. Neue Funktionen entstehen möglichst mit den vorhandenen Mitteln der IAM-Software.
- Erweiterbare Basis: Zusätzliche Schnittstellen und Governance-Funktionen lassen sich ergänzen, ohne Sonderlogik fortzuschreiben.

Die Umstellung war für die Anwender:innen nicht in jedem Punkt sofort selbstverständlich. Vor allem die neue Oberfläche galt in den Fachbereichen und Kliniken zunächst als gewöhnungsbedürftig. Mit zunehmender Nutzung zeigte sich, wie viele Abläufe automatisiert ablaufen, und die Akzeptanz nahm zu. Innerhalb der IT kam die neue Plattform von Beginn an gut an.

Ausblick: Die IAM-Plattform entwickelt sich weiter

Nach dem Rollout folgte zunächst die Stabilisierung. Seitdem baut HOCH die Umgebung schrittweise aus. Dazu gehören Schnittstellen zu SAP Cloud, zum Lernmanagementsystem (LMS) und zu Microsoft Entra ID sowie eine Rezertifizierungslösung für Admin-Accounts.

Als nächste Themen stehen PAM und VAM auf der Roadmap. Der Ausbau folgt dem Prinzip der Erneuerung: neue Anforderungen möglichst nah am Produktstandard umsetzen.



Fazit: Modernisierung beginnt beim Daten- und Rollenmodell

Der Wechsel der IAM-Plattform war für HOCH nur ein Teil der Aufgabe. Entscheidend war, ein über Jahre individualisiertes Daten- und Rollenmodell neu zu ordnen.

Mit OpenText Identity Manager und Identity Governance verfügt HOCH über eine Basis, auf der HR-Informationen die Rollen- und Rechtevergabe steuern und Sonderlogik die Ausnahme bleibt.