AIRLOCK®
SECURE ACCESS HUB

HIN

Modernisierung der Sicherheitsarchitektur mit Airlock Microgateway

Health Info Net AG (HIN)



Im Gesundheitswesen sind die Anforderungen an den Schutz sensibler Daten besonders hoch. Deshalb legen wir bei der Wahl unserer Technologiepartner grossen Wert auf Sicherheit, digitale Souveränität und langfristige Verlässlichkeit. Bei Airlock Microgateway schätzen wir, dass mit Ergon ein Zürcher Unternehmen hinter der Lösung steht, das über lange Erfahrung im Schweizer Banking- und Public-Sector-Umfeld verfügt.

Mohammad Alavi, CTO bei HIN

Die Health Info Net AG (HIN) verbindet seit 1996 Akteure im Schweizer Gesundheitswesen sicher miteinander. Als die historisch gewachsene Infrastruktur den steigenden Anforderungen an Flexibilität, Automatisierung und Unabhängigkeit nicht mehr gerecht wurde, entschied sich HIN für eine Neuausrichtung. Gemeinsam mit spezialisierten Partnern entstand eine Kubernetes-native, GitOps-basierte Architektur auf offenen Standards – mit Airlock Microgateway als zentralem Baustein für den Schutz von Webapplikationen und APIs.

Ein Netzwerk, dem die Schweiz vertraut

Über 50 000 Fachpersonen und Institutionen – darunter Spitäler, Praxen, Apotheken, Labore, Versicherer und Behörden – nutzen HIN für den sicheren Austausch sensibler Gesundheitsdaten.

Wo der Schutz von Gesundheitsdaten zum Kerngeschäft gehört, sind Sicherheit und Verfügbarkeit nicht verhandelbar. Gleichzeitig muss die Infrastruktur mit neuen digitalen Services und steigenden Anforderungen Schritt halten. Genau hier setzte die Modernisierung an.

Wenn Legacy-Infrastruktur an ihre Grenzen stösst

Die bestehende Infrastruktur hatte sich über viele Jahre bewährt. Mit der Weiterentwicklung der digitalen Services stiegen jedoch die Anforderungen an Flexibilität, Automatisierung und Skalierbarkeit. Änderungen an der Infrastruktur waren aufwendig, neue Services liessen sich nicht mehr im gewünschten Tempo bereitstellen. Die Umsetzung über Tickets dauerte teilweise mehr als zwei Wochen, während zahlreiche individuelle Lösungen den Wartungs- und Aktualisierungsaufwand erhöhten.

Auch die vorgelagerte Sicherheitsarchitektur war über Jahre gewachsen und entsprechend komplex. Neue Anforderungen liessen sich nur mit hohem Aufwand umsetzen. Gleichzeitig wollte HIN Entwicklungsteams mehr Eigenständigkeit geben, Prozesse stärker automatisieren und die Abhängigkeit von einzelnen Technologien und Infrastrukturprovidern reduzieren.

Die zentralen Herausforderungen waren:

- **Eingeschränkte Anpassbarkeit:** Statische Konfigurationen und aufwendige Änderungen erschwerten agile Deployment-Zyklen.
- **Hohe Sicherheits- und Compliance-Anforderungen:** Granulare Sicherheitsrichtlinien für sensible Gesundheitsdaten liessen sich manuell nicht mehr effizient skalieren.
- **Technologische Abhängigkeiten:** Spezifische Proxy-Logiken und Hosting-Strukturen schränkten die strategische Handlungsfreiheit ein.
- **Verteilte Verantwortlichkeiten:** Infrastruktur-, Plattform-, Security- und Applikationsteams benötigten ein Betriebsmodell, das ihre Aufgaben klar voneinander trennt.

Für HIN war deshalb klar, dass es mehr brauchte als den Austausch einzelner Komponenten: eine grundlegende Modernisierung der Sicherheits- und Betriebsarchitektur.

Projekt Phoenix: Leitprinzipien für die neue Plattform

Mit dem *Projekt Phoenix* leitete HIN diese Neuausrichtung ein. Inspiriert vom Buch The *Phoenix Project*[1] entstand das Ziel, eine standardisierte, automatisierte und widerstandsfähige Plattform aufzubauen, in der Entwicklung, Betrieb und Sicherheit eng zusammenarbeiten.

1 The Phoenix Project: Ein Roman über IT, DevOps und wie Sie Ihr Unternehmen zum Erfolg führen von Gene Kim (Autor), Kevin Behr (Autor), George Spafford (Autor)

Sechs Leitprinzipien prägten das Vorhaben:

1. **GitOps und Nachvollziehbarkeit:** Änderungen sollten zentral dokumentiert, versioniert und revisionssicher nachvollziehbar werden.
2. **Security First:** Datenschutz, Compliance und Sicherheit sollten von Anfang an berücksichtigt werden.
3. **Dual-Vendor-Strategie:** Abhängigkeiten sollten reduziert und die Widerstandsfähigkeit erhöht werden.
4. **Offene Standards:** Proprietäre Insellösungen sollten durch standardisierte, portable Ansätze ersetzt werden.
5. **Automatisierung und Agilität:** Wiederholbare Prozesse sollten den Betrieb vereinfachen und neue Services schneller ermöglichen.
6. **Schnellere Time-to-Market:** Neue Services sollten schneller und kosteneffizienter bereitgestellt werden..

Damit verband HIN die technische Modernisierung mit einem übergeordneten Ziel: mehr Kontrolle über Infrastruktur und Betriebsprozesse.

Ein Partner-Ökosystem mit klaren Aufgaben

Aus diesen Anforderungen ergab sich das Zielbild einer Kubernetes-Plattform, die sich automatisiert betreiben lässt, hohe Sicherheitsanforderungen erfüllt und nicht von einem einzelnen Anbieter abhängt.

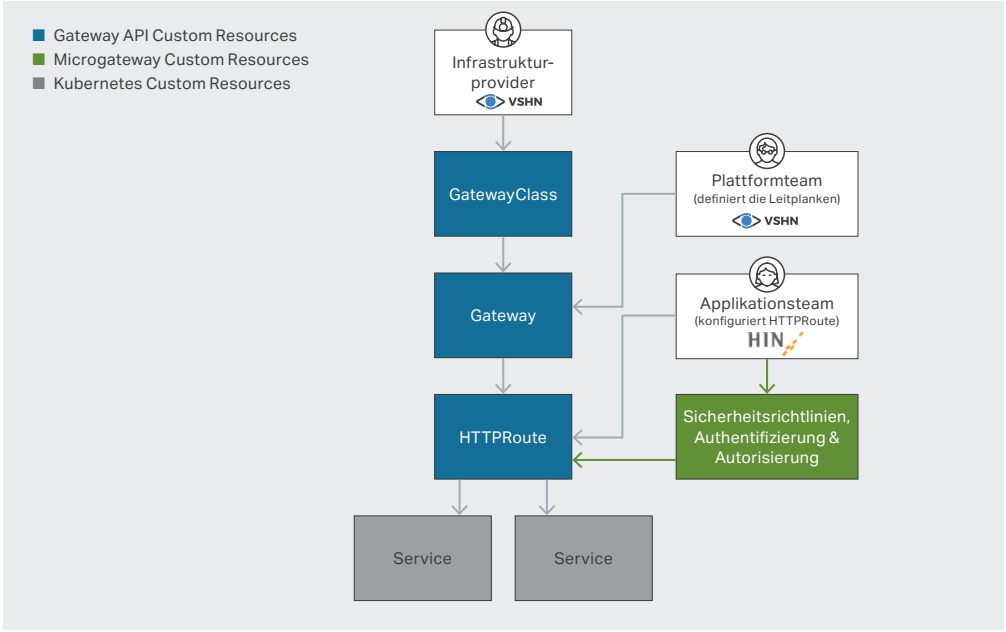
Dafür setzt HIN bewusst auf spezialisierte Partner. Red Hat OpenShift bildet die Kubernetes-Plattform, VSHN verantwortet deren Betrieb und unterstützt HIN bei Architektur und Migration. Mit cloudscale.ch und Exoscale nutzt HIN zwei unabhängige Cloud-Provider. Dadurch reduziert das Unternehmen die Abhängigkeit von einem einzelnen Infrastrukturprovider und erhöht die Resilienz der Plattform. Airlock übernimmt mit dem Microgateway den Kubernetes-nativen Schutz der Webapplikationen und APIs. Weitere Technologiepartner sind in die Identitäts- und Authentisierungsarchitektur eingebunden.

Auch innerhalb der Plattform sind die Aufgaben klar verteilt. Das Ressourcen- und Rollenmodell der Kubernetes Gateway API unterstützt diese Aufgabenteilung.

> ***Die klare Rollenteilung der Gateway API konnten wir mit Airlock Microgateway konsequent umsetzen. Über das deklarative Konfigurationsmodell definiert das Plattformteam die Leitplanken, während die Applikationsteams ihre Routen und Security-Policies selbst verwalten. Das vereinfacht die Zusammenarbeit über mehrere Teams und Partner hinweg und macht den Betrieb effizienter.***



Andreas Gruhler,
Cloud Architect bei HIN



Rollenorientiertes Betriebsmodell auf Basis der Kubernetes-Gateway-API. VSHN stellt die Plattform und die Gateways bereit, wobei Airlock Microgateway als Implementierung der Gateway-API dient, während HIN die Routen und Sicherheitsrichtlinien verwaltet.

Warum sich HIN für Airlock Microgateway entschied

Für den Schutz ihrer Webapplikationen und APIs suchte HIN eine Lösung, die sich in OpenShift, das GitOps-basierte Betriebsmodell und die bestehende IAM-Landschaft integrieren liess und zugleich genügend Spielraum für spezifische Anforderungen bot. Konfigurationsänderungen sollten ohne Neustart übernommen werden können, und auch die Security-Komponente musste zum verteilten Betriebsmodell von HIN und ihren Partnern passen.

Airlock Microgateway erfüllte diese Anforderungen als Kubernetes-native Implementierung der Gateway API. Für das Routing setzt HIN damit auf das standardisierte Ressourcenmodell der Kubernetes Gateway API statt auf ein proprietäres Routing-Modell. Die Lösung ergänzt dieses um Web Application and API Protection und identitätsbasierte Zugriffskontrolle und ist für Red Hat OpenShift zertifiziert.

Für die Dual-Vendor-Strategie von HIN ist zudem entscheidend, dass die Security-Architektur nicht an einen bestimmten Cloud-Provider gekoppelt ist. Als Cloud-agnostische, Kubernetes-native Lösung lässt sich Airlock Microgateway konsistent in den OpenShift-Umgebungen von HIN betreiben. Damit bleibt auch die Security-Schicht über unterschiedliche Cloud-Infrastrukturen hinweg portabel.

Die bestehende Identity-Infrastruktur lässt sich über Standards wie OIDC integrieren. OAuth 2.0 Token Exchange sowie Erweiterungsmöglichkeiten über ICAP oder LUA ermöglichen darüber hinaus die Umsetzung spezifischer Anforderungen.

Wie HIN Routing, Applikationsschutz und Identität zusammenführt

HIN nutzt Airlock Microgateway in der neuen Architektur für drei zentrale Aufgaben. Am Einstieg in den Cluster führt die Lösung Routing, Applikationsschutz und identitätsbasierte Zugriffskontrolle in einer Kubernetes-nativen Komponente zusammen.

- **Routing mit Gateway API:** HIN definiert die Routen ihrer Anwendungen über das standardisierte Ressourcenmodell der Kubernetes Gateway API. Airlock Microgateway setzt diese Konfiguration um und steuert, welcher Traffic zu welchem Service gelangt.
- **Web Application and API Protection:** Starke Security-Defaults schützen Webapplikationen und APIs von Beginn an, unter anderem vor bekannten Angriffsmustern der OWASP Top 10.
- **Identity-aware Proxy:** Für interaktive Browserzugriffe fungiert Airlock Microgateway als OIDC Relying Party und integriert sich damit über einen etablierten Standard in die bestehende Identity-Infrastruktur von HIN. Gleichzeitig ermöglicht die Integration ein durchgängiges Single Sign-on.

  Für HIN ist diese Funktion besonders relevant: Neben klassischen Browserzugriffen muss die Plattform auch Drittapplikationen und technische Geräte absichern. Bei OAuth-basierten Zugriffen nimmt Airlock Microgateway das mitgelieferte Access Token entgegen und kann über OAuth 2.0 Token Exchange ein Token für den Zugriff auf den nachgelagerten Service beziehen.

  Für besonders sensible Anwendungen oder Pfade kann HIN zudem ein höheres Authentisierungsniveau verlangen. Bereits authentisierte Benutzer:innen werden dann gezielt zu einem zusätzlichen Authentisierungsschritt weitergeleitet. Erst wenn das erforderliche Vertrauensniveau erreicht ist, wird der Zugriff auf die geschützte Ressource freigegeben.

> ***Entscheidend war für uns die Kombination aus Standardisierung und Erweiterbarkeit: Airlock Microgateway baut auf der Kubernetes Gateway API auf, integriert sich nativ in OpenShift und unterstützt unsere IAM-Integration über offene Standards wie OIDC und OAuth 2.0 Token Exchange. Gleichzeitig können wir sehr spezifische Anforderungen umsetzen, wie etwa mit ICAP für Malware-Scanning oder Lua.***



Andreas Gruhler,
Cloud Architect bei HIN

Sicherheitsrichtlinien werden Teil des Entwicklungsprozesses

Ein zentraler Vorteil der neuen Architektur ist die deklarative Konfiguration. Routen und Sicherheitsrichtlinien werden in Git verwaltet, versioniert, geprüft und automatisiert ausgerollt. Damit fügt sich Airlock Microgateway konsequent in das DevSecOps-Modell von HIN ein: Sicherheit wird als Code direkt in Entwicklungs- und Betriebsprozesse integriert.

Änderungen bleiben dadurch nachvollziehbar und können vor dem Rollout geprüft und freigegeben werden. Test-, Pre-Production- und Produktivumgebungen lassen sich nach denselben Prinzipien betreiben, während Rollouts kontrolliert automatisiert werden können.

Auch die Migration der bestehenden Konfigurationen folgt diesem Ansatz. Ein eigens entwickeltes Skript überführt bestehende Konfigurationen automatisiert in Gateway-API- und Microgateway-Manifest, die anschliessend über ArgoCD ausgerollt werden. Die schrittweise Überführung und begleitende End-to-End-Tests ermöglichten es HIN, die geschäftskritische Umgebung kontrolliert zu modernisieren, ohne die gesamte Umgebung auf einmal umstellen zu müssen.

Von der Migration zum modernen Plattformbetrieb

Die Modernisierung verändert nicht nur die Technologie, sondern auch die Art, wie HIN ihre digitale Plattform entwickelt und betreibt.

- **Mehr Kontrolle und Resilienz:** HIN kann ihre Anwendungen auf zwei unabhängigen Cloud-Infrastrukturen betreiben. Die Security-Schicht bleibt dabei Cloud-unabhängig und lässt sich in beiden OpenShift-Umgebungen nach denselben Prinzipien einsetzen.
- **Mehr Sicherheit:** Airlock Microgateway setzt Applikationsschutz und identitätsbasierte Zugriffskontrolle direkt vor den Services durch. Funktionen wie Step-up-Authentisierung ermöglichen zusätzliche Schutzstufen für besonders sensible Zugriffe.
- **Mehr Effizienz und Agilität:** Automatisierung und «Security Policy as Code» beschleunigen Deployments – von mehreren Stunden auf wenige Minuten.
- **Mehr Freiraum für Entwicklung:** Die gelebte DevOps-Kultur mit klar verteilten Verantwortlichkeiten entlastet Entwicklungsteams von Routineaufgaben und unterstützt die schnellere Weiterentwicklung digitaler Services.

Das Fundament für die nächsten digitalen Gesundheitsservices

Mit der neuen Plattform hat HIN ihre Sicherheitsarchitektur grundlegend neu ausgerichtet. Offene Standards, klare Verantwortlichkeiten und automatisierte Prozesse schaffen eine Umgebung, die sich flexibel weiterentwickeln lässt und Abhängigkeiten von einzelnen Technologien und Anbietern reduziert.

Airlock Microgateway fügt Applikationsschutz und identitätsbasierte Zugriffskontrolle direkt in dieses Kubernetes-native Betriebsmodell ein. So wird Sicherheit zum festen Bestandteil von Entwicklung und Betrieb.

HIN schafft damit eine flexible und automatisierbare Grundlage, um digitale Gesundheitsservices auch künftig sicher weiterzuentwickeln.

> ***Airlock Microgateway hat uns überzeugt, weil die Lösung unsere Security-Prinzipien ideal unterstützt und gleichzeitig konsequent auf containerbasierte Architekturen ausgerichtet ist. Die cloud-native und skalierbare Architektur sowie die enge technische Zusammenarbeit waren für uns zentrale Faktoren.***



Mohammad Alavi,
CTO bei HIN

Über Health Info Net AG (HIN)

Die Health Info Net AG (HIN) wurde 1996 von Ärzten für Ärzte gegründet. Heute unterstützt HIN Gesundheitsfachpersonen und -institutionen in der Schweiz mit digitalen Services für eine einfache, sichere und datenschutzkonforme Kommunikation und Zusammenarbeit. Bekannt ist die Plattform insbesondere durch HIN Mail, über das jährlich Millionen verschlüsselter E-Mails versendet werden. HIN schützt sensible Gesundheitsdaten, stellt deren Verfügbarkeit sicher und trägt damit zur digitalen Souveränität im Schweizer Gesundheitswesen bei. Ziel ist es, administrative Abläufe zu vereinfachen und Gesundheitsfachpersonen mehr Zeit für ihre Patientinnen und Patienten zu ermöglichen.

Über Airlock – Security Innovation by Ergon Informatik AG

Der Airlock Secure Access Hub vereint die wichtigen IT-Sicherheitsthemen der Filterung und Authentisierung zu einem gut abgestimmten Gesamtpaket, das Massstäbe in Sachen Bedienbarkeit und Services setzt. Der Secure Access Hub deckt alle wichtigen Funktionen der modernen IT-Sicherheit in diesem Bereich ab: von einer durch Fachjournalisten ausgezeichneten Web Application Firewall (WAF), über ein Customer Identitäts- und Zugriffsmanagement (cIAM), dem Schweizer Banken vertrauen, hin zu einer API-Sicherheit, die neueste Anforderungen stemmt. Die IT-Sicherheitslösung Airlock schützt mehr als 20 Millionen aktive, digitale Identitäten und 30.000 Back-Ends von über 550 Kunden auf der ganzen Welt. Weitere Informationen unter www.airlock.com. Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG.

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für den Erfolg sind 300 hochqualifizierte IT-Spezialisten, die dank herausragendem Fachwissen neue Technologietrends schnell antizipieren und mit innovativen Lösungen entscheidende Wettbewerbsvorteile sicherstellen. Ergon Informatik realisiert hauptsächlich Grossprojekte im Bereich B2B.

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich
+41 44 268 89 00
info@airlock.com

airlock.com

ergon

Copyright © 2026 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries. Other products or trademarks mentioned are the property of their respective owners.