SUCCESS STORY

FLUGHAFEN MÜNCHEN GMBH

Ein starker Partner der Region

Der Flughafen München ist der zweitgrößte Airport in Deutschland und wird von knapp 90 Fluggesellschaften angeflogen. Mit rund 33.000 Beschäftigten bei knapp 500 Unternehmen zählt er zu den größten Arbeitsstätten Bayerns. Betreiberin des Airports ist die Flughafen München GmbH (FMG), die alleine 8.700 Mitarbeitende beschäftigt.

KOMMUNIKATION IN VIRTUELLEN DIALOGRÄUMEN

Im April 2022 hat die Flughafen München GmbH ein konzernweites Social Intranet als neue digitale Heimat eingeführt und das bisherige Intranet abgelöst. Erstmals können alle Mitarbeitenden des Flughafens und ihrer Tochter- und Beteiligungsgesellschaften gemeinsam eine moderne Plattform zur Information, Kommunikation und Kollaboration nutzen.

Das Social Intranet bietet neben allen relevanten Konzernnachrichten auch die Möglichkeit, sich über einen integrierten Chat und Communities team- und hierarchieübergreifend auszutauschen. Um innerhalb des Systems kommunizieren und agieren zu können, haben alle Mitarbeitenden ein eigenes Benutzerprofil, eine Art digitale Visitenkarte. So können sie unter ihrem Namen Beiträge verfassen und kommentieren oder im Chat mit anderen Nutzenden Nachrichten schreiben.

Das Accountmanagement erfolgt über die eingesetzte Identity & Access Management Software SecuIAM vom Hersteller OEDIV SecuSys GmbH.

Dabei werden Accounts in einem für diesen Zweck bereitgestellten LDAP-Server erstellt. Die Verwaltung der Accounts wurde mithilfe von SecuIAM soweit automatisiert, dass für neue Mitarbeitende zum Eintrittsdatum Zugänge eingerichtet werden und beim Austritt die Accounts wieder gelöscht werden.

Für die Verwaltung der Communities werden den Mitarbeitenden in SecuIAM Rollen zugewiesen, die aufgrund der Zuordnung zu Organisationseinheiten entsprechende Berechtigungen einräumen.

> *„Während des Projekts wurde nicht nur die LDAP-Schnittstelle zur Userverwaltung geschaffen, sondern auch noch weitere – zum Beispiel um Telefonnummern der Mitarbeitenden verarbeiten zu können und um weitere Quellen für HR-Daten zu integrieren.*
>
> *(Marcel Michelmann, Servicebereich IT, Flughafen München GmbH)*

ZIEL

- Implementierung einer konzernweiten Kommunikationsplattform
- Schneller orts- und zeitunabhängiger Zugriff auf Informationen
- Automatisierung der Nutzer- und Berechtigungsverwaltung
- Nutzung des Social Intranets über eine Desktop-App oder mobile App

PROJEKTÜBERSICHT

- Integration einer LDAP-Schnittstelle zur Accountprovisionierung
- Integration einer Schnittstelle für HR-Daten
- Planung von Rollen- und Prozessmodellen
- Erweiterung des Organisationsmodells
- Anreicherung der Kommunikationsdaten aus unterschiedlichen Quellen

ERFOLG

- Konzernweite Vernetzung aller Mitarbeitenden übers Social Intranet
- Verfassen von Beiträgen und Postings durch jeden User möglich
- Automatisierte Accountverwaltung (Mitarbeitereintritt und -austritt)
- Zielgerichtete Migration aus dem HR-System mittels Input-Connector für SAP HCM

WARUM IT-SECURITY?

Das Thema IT-Security hat in den letzten Jahren enorm an Bedeutung gewonnen. Nicht nur zahlreiche Fälle von Datenmissbrauch, Cyberangriffen und Hacking sensibilisieren gleichermaßen Unternehmen sowie die Öffentlichkeit für das Thema. Auch die gestiegene Digitalisierung und Zunahme von hybriden Betriebsszenarien machen eine Auseinandersetzung mit grundlegenden Fragen zum Umgang mit Daten und digitalen Systemen dringend erforderlich.

HERAUSFORDERUNGEN KRITIS

Organisationen, die zu kritischen Infrastrukturen zählen, sind von besonderer Bedeutung für die Grundversorgung eines Landes und seiner Bevölkerung. Daher unterliegen sie durch das IT-Sicherheitsgesetz 2.0 speziellen Auflagen, durch die eine frühzeitige Risikoerkennung erzielt und mittels technologischer Maßnahmen Betriebsausfälle vermieden werden sollen. Eine wesentliche Rolle spielt hierbei die Sicherstellung authentifizierter Zugriffsrechte, um sensible Daten zu schützen.

> *Wir kennen die besonderen Sicherheitsanforderungen des BSI-Gesetzes an KRITIS-Organisationen. SecuIAM kann das Schutzlevel der komplexen IT-Systeme erhöhen, um so eine 24/7-Betriebsbereitschaft zu ermöglichen. (Fabian Neumann, Geschäftsführer, OEDIV SecuSys GmbH)*

WAS IST IAM?

Identity & Access Management (IAM) versetzt Unternehmen in die Lage, die Zugriffsberechtigungen und -voraussetzungen ihrer Mitarbeitenden effizient zu managen. Häufig betrifft dies ebenso externe Zugriffe durch Partner-, Lieferanten- oder Kundenunternehmen.

Kurzum: IAM sorgt für die Autorisierung und Authentisierung, hilft beim Einhalten von Compliance-Vorgaben und sorgt für die Verwaltung und das Monitoring aller digitalen Identitäten.

ÜBER UNS

Die OEDIV SecuSys GmbH entwickelt seit 1998 branchenneutrale Softwarelösungen rund um Identity & Access Management. Konkret geht es um die Entwicklung neuer Lösungen für die wachsenden Herausforderungen der prozessgestützten Verwaltung von Identitäten und Zugriffsberechtigungen sowie die steigenden Anforderungen in den Bereichen Security, Risk und Compliance. OEDIV SecuSys ist ein Tochterunternehmen der OEDIV Oetker Daten- und Informationsverarbeitung KG und ein Teil der international agierenden Oetker-Gruppe.

ANSCHRIFT

OEDIV SecuSys GmbH
Brückenweg 5
18146 Rostock

KONTAKT

Tel. +49 381 37573-0
Fax +49 381 37573-29
vertrieb@secusys.de

MEHR INFOS

www.secusys.de