



Höhere Sicherheit und Compliance mit IAM bei der KGAL GmbH & Co. KG

Führender deutscher Real Asset Manager sichert
Zugriffsrechte auf kritische Anwendungen mit dem
Garancy Identity Manager

Ein Produkt von  beta systems





Das Unternehmen

Die KGAL gehört zu den führenden deutschen Real Asset Managern und verwaltet Investitionen in den Bereichen Immobilien, nachhaltige Infrastruktur und Aviation. Das Unternehmen mit Sitz in Grünwald bei München betreut institutionelle und private Investoren und verwaltet ein Investitionsvolumen von rund 16 Milliarden Euro.



● DIE HERAUSFORDERUNG

Manuelle Einzelprozesse ersetzen

Bei der KGAL unterstützte eine bestehende Eigenentwicklung zwar Standardprozesse rund um Ein- und Austritte, stieß jedoch bei Rollenverwaltung, Rezertifizierungen und einer zentralen Governance an ihre Grenzen. Manuelle Abläufe über Excel und Tickets verursachten hohen Aufwand, erschwerten die Nachvollziehbarkeit und erhöhten den Abstimmungsbedarf zwischen Fachbereichen und IT.

● DIE LÖSUNG

Identity Governance zentral neu aufgestellt

Gemeinsam mit Garancy führte die KGAL den Identity Manager als zentrale Plattform für die Berechtigungsverwaltung ein. Ein umfassendes Rollenmodell mit Basis-, Organisations-, Funktions- und Fachrollen bildet heute die Grundlage der Rechtevergabe. Standardprozesse wurden automatisiert, bestehende Systeme angebunden und Rezertifizierungen in einen zentralen Workflow integriert. Gleichzeitig wurden die Verantwortlichen so befähigt, viele Anpassungen selbst vorzunehmen.

● DAS ERGEBNIS

Mehr Sicherheit, Transparenz und Effizienz

Heute verwaltet die KGAL Berechtigungen zentral und nachvollziehbar. Automatisierte Joiner-, Mover- und Leaver-Prozesse entlasten die IT, Rezertifizierungen lassen sich deutlich einfacher durchführen und Compliance-Anforderungen werden zuverlässig unterstützt. Gleichzeitig sorgt die zentrale Verwaltung für mehr Transparenz über bestehende Berechtigungen und reduziert das Risiko unbefugter Zugriffe.

Eine zentrale IAM-Lösung ist ein wichtiger Baustein für eine moderne und sichere IT. Unternehmen, die ihre Berechtigungsverwaltung professionalisieren wollen, sollten sich daher intensiv mit dem Thema Identity Management auseinandersetzen. Wir haben mit Garancy die richtige Wahl getroffen.



Ludwig Eggersdorfer

Head of Digital Workplace, IT-Governance & Infrastructure Solutions

Technologie, Prozesse und Rollen perfekt verzahnt

Out-of-the-Box-Funktionen

Die Eigenentwicklung („Mitarbeiter Hub“) deckte Standardprozesse wie Zugang, Abgang und Änderungen von Beschäftigtenverhältnissen und ihre Auswirkung auf die Zugangsberechtigungen ab, aber nur unzureichend die Themen Rollenvergabe und wiederkehrende Rezertifizierung. Auf der Suche nach einer professionellen Lösung fiel die Wahl nach sorgfältiger Evaluierung verschiedener Anbieter 2022 auf den Garancy Identity Manager. Seit Juli 2023 ist er im Echtbetrieb.

Bernd Stiller, Projektleiter im Bereich Digital Workplace, erzählt: „Als mittelständisches Unternehmen arbeiten wir mit einem Technologiepartner gerne auf Augenhöhe zusammen und mit festen Kontaktpersonen, die auf Anfragen schnell reagieren. Natürlich muss auch die Software zu uns und unseren Anforderungen passen.“ Er hebt insbesondere die Möglichkeit zur Rezertifizierung von Berechtigungen mit Garancy hervor.

Der Identity Manager bietet zudem Out-of-the-Box-Funktionen zur Abbildung von Standardprozessen wie Mitarbeiter Eintritt und -austritt sowie Abteilungswechsel und lässt sich sehr flexibel an individuelle Bedürfnisse anpassen.

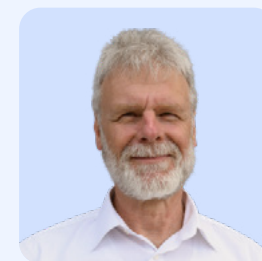
Ludwig Eggersdorfer, Head of Digital Workplace, IT-Governance & Infrastructure Solutions, ergänzt: „Garancy als deutschem Anbieter sind die regulatorischen Anforderungen der Branche wie u. a. der BaFin vertraut. Das ist für uns enorm wichtig.“

Systemanbindung über uConnect

Die Konnektortechnologie von Garancy ermöglicht eine unkomplizierte Anbindung aller bei der KGAL vorhandenen Systeme an den Identity Manager. Viele Applikationen basieren mit ihren Rechten auf Gruppen im Active Directory. Diese Rechte werden nach Genehmigung in Garancy automatisch zugeteilt.

Bei anderen Applikationen müssen bestellte Rechte manuell eingetragen werden. Über die Anbindung des Ticketsystems werden entsprechende Tickets zur Erteilung der Rechte ausgelöst und nachgehalten. Die bestellbaren Rechte sind verständlich für Anwender formuliert. Es gibt somit keine Missverständnisse mehr zwischen Bestellung durch die Anwender und Erteilung der Rechte durch die IT. Unnötige Nacharbeiten und Medienbrüche entfallen.

Als mittelständisches Unternehmen arbeiten wir mit einem Technologiepartner gerne auf Augenhöhe zusammen, mit festen Kontaktpersonen, die bei Anfragen schnell reagieren.



Bernd Stiller
Projektleiter Digital Workplace

Rollenkonzept – die Basis der Berechtigungsverwaltung

Ein wichtiger Baustein für die erfolgreiche Implementierung des Garancy Identity Managers ist immer ein durchdachtes Rollenkonzept, so auch bei der KGAL. In Ansätzen war es bereits vor Garancy vorhanden, mit dem Projekt wurde es aber erst richtig ausgestaltet und umfasst heute vier Rollentypen:

- **Basisrollen** werden allen internen und externen Beschäftigten automatisch zugewiesen und beinhalten grundlegende Berechtigungen, die für alle erforderlich sind.
- **Organisationsrollen** erhalten Personen anhand ihrer Organisationseinheit. Sie enthalten Berechtigungen, die zum Ausüben ihrer Tätigkeit in dieser Einheit erforderlich sind.
- **Funktionsrollen** werden Personen basierend auf ihrer Funktion zugewiesen und umfassen zusätzliche Berechtigungen.
- **Fachrollen** werden für spezifische Aufgaben und Verantwortlichkeiten vergeben, etwa an externe Dienstleister wie Wirtschaftsprüfer und Steuerberater.

Über das Recertification Center können wir den Fortschritt der Aktualisierungen wesentlich besser überwachen, über den einzelnen Beschäftigten in das System gehen und seine Rechte überprüfen.



Sabine Mehner
Vendor Management

Sabine Mehner aus dem Vendor Management ist für die Bestellung und Verwaltung der Rechte der externen Dienstleister zuständig und kann über das Fachrollen-Konzept Zugriffe sehr granular steuern. Begeistert ist sie explizit von der einfacheren Rezertifizierung von Berechtigungen.

Vor der IAM-Einführung war dies ein zeitaufwändiger und fehleranfälliger Prozess, organisiert über Excel und Ticketsysteme. Sie erhielt für jede Applikation eine Liste mit den Namen derjenigen, die darauf Zugriff haben. Diese musste sie Zeile für Zeile bearbeiten und konnte dies mitunter auch nur nach individuellen Rücksprachen tun. „Das zog sich manchmal über ein, zwei Wochen hin“, erzählt sie.

Über das Recertification Center kann Sabine Mehner heute den Fortschritt der Aktualisierungen wesentlich besser überwachen. Sie kann über den einzelnen Beschäftigten in das System gehen und dessen Rechte prüfen – unabhängig für welche Applikation. „Es ist immer noch Arbeit, aber eben ein deutlich geringerer Aufwand“, sagt sie.

Partnerschaftlicher Ansatz

Die Zusammenarbeit mit Garancy beurteilen die Verantwortlichen bei der KGAL als durchweg positiv. „Wir haben uns von Haus aus auf die Fahne geschrieben, uns selbst sehr tief in das System einzuarbeiten. Dadurch müssen wir nicht jeden Auftrag an Garancy vergeben. Hierbei hat uns der Hersteller sehr gut unterstützt und steht auch sonst bei Bedarf mit Rat und Tat zur Seite,“ berichtet Bernd Stiller. Bei größeren Projekten oder Änderungswünschen setzt man sich zusammen und erarbeitet gemeinsam eine Lösung – ein partnerschaftlicher Ansatz mit offenem Austausch.

Fazit: IAM als Baustein für eine sichere IT

Die Einführung des Garancy Identity Managers war für die KGAL eine Investition, die sich in vielerlei Hinsicht ausgezahlt hat. Durch die zentrale Verwaltung der Berechtigungen konnte das Unternehmen seine IT-Sicherheit deutlich verbessern und das Risiko von unbefugten Zugriffen reduzieren.

Die Lösung unterstützt die Einhaltung von Compliance-Anforderungen, vor allem im Hinblick auf die Rezertifizierung von Berechtigungen. Durch Automatisierung von Standardprozessen (Joiner, Mover, Leaver) arbeitet die IT-Abteilung deutlich effizienter. Zudem ist die Transparenz gestiegen, denn die zentrale Verwaltung ermöglicht einen besseren Überblick über die vorhandenen Berechtigungen und erleichtert die Überwachung von deren Einhaltung.

„Eine zentrale IAM-Lösung ist ein wichtiger Baustein für eine moderne und sichere IT. Unternehmen, die ihre Berechtigungsverwaltung professionalisieren wollen, sollten sich daher intensiv mit dem Thema Identity Management auseinandersetzen. Wir haben mit Garancy die richtige Wahl getroffen“, sagt Ludwig Eggersdorfer.

Die wichtigsten Fakten

● GRÜNDUNGSJAHR

1968

● BESCHÄFTIGTE

ca. 400

● HAUPTSITZ

Grünwald bei München

● BRANCHE

Finanzdienstleistungen /
Asset Management

Die KGAL investiert seit Jahrzehnten in reale Vermögenswerte und verbindet langfristige Anlagestrategien mit hohen regulatorischen Anforderungen.

Der Erfolg dank Garancy

- Automatisierte Joiner-, Mover- und Leaver-Prozesse
- Flexible Rollenmodelle für interne Mitarbeitende und externe Dienstleister
- Deutlich vereinfachte Rezertifizierung von Berechtigungen
- Weniger manueller Aufwand für IT und Fachbereiche
- Höhere Transparenz, Compliance und Nachvollziehbarkeit
- Eigenständige Administration vieler Anpassungen ohne Herstellerunterstützung

Produkte im Einsatz bei der KGAL

- Garancy Identity Manager
- Garancy User Center
- Garancy Recertification Center
- ConPack
- uConnect Advanced

Wann starten Sie Ihr Erfolgsprojekt?

Lassen Sie uns über Ihre Möglichkeiten mit Garancy sprechen!

✉ hello@garancy.com

☎ +49 (0) 30 726 118-0