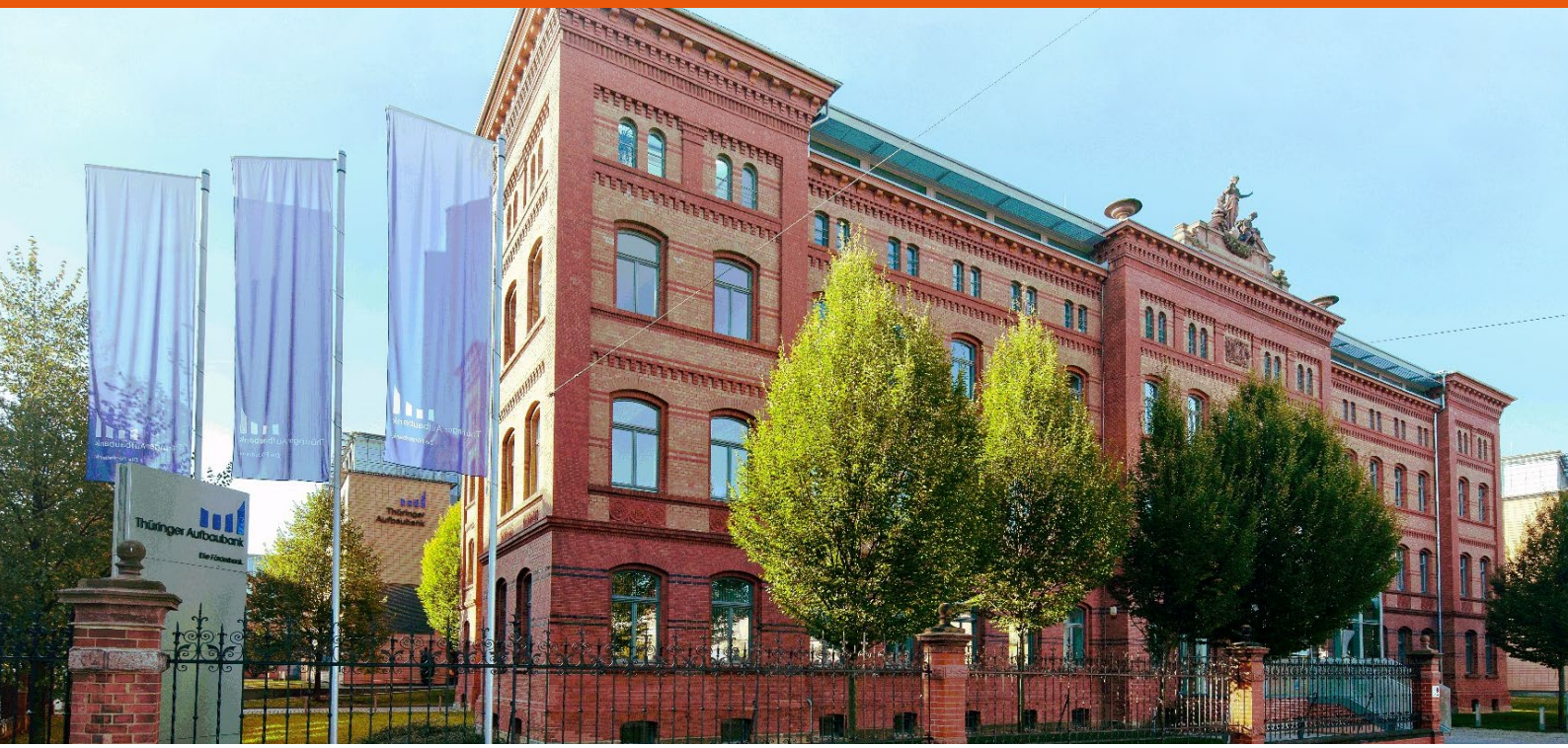
_betasystems



EINFÜHRUNG EINER NEUEN IAM-LÖSUNG BEI DER THÜRINGER AUFBAUBANK

Referenzprojekt

Thüringer Aufbaubank

Die Förderbank.

Die regulatorischen Anforderungen der MaRisk nehmen eher zu denn ab. Mit ihrer bisherigen IAM-Lösung konnte die Thüringer Aufbaubank diese nicht mehr bewältigen. Deshalb hat das Unternehmen im Jahr 2019 einen Schwenk vollzogen und arbeitet jetzt mit dem GARANCY Identity Manager. Er erlaubt insbesondere die vorher nur wenig praktizierte Umsetzung eines Rollenkonzeptes, mit dem sich das Prinzip „Kein Recht ohne Rolle" konsequent anwenden lässt.

Die Tage des Laufzettels, auf dem ausgeführt wurde, wer wann welche Berechtigung in welchem IT-System benötigt, sind bei der Thüringer Aufbaubank (TAB) schon lange vorbei. Circa 800 Beschäftigte zählt die Förderbank inklusive Tochtergesellschaften, die größtenteils am Hauptstandort Erfurt arbeiten. Bereits 2016 hatte die Aufbaubank im Rahmen eines IT-Governance-Projektes ein Tool zur zentralen Identitäts- und Berechtigungsverwaltung eingeführt. Nach einem Jahr Betrieb und mit Blick auf die Entwürfe der MaRisk und der BAIT wurde jedoch deutlich: Die Software würde den steigenden regulatorischen Anforderungen in der damaligen Ausprägung auf Dauer nicht genügen.

Eine Prüfung nach §44 KWG, angeordnet von der BaFin und durchgeführt durch Prüfer*innen der Bundesbank, bestätigte die Meinung der TAB und gab den endgültigen Anstoß: Das bisherige IAM-Konzept sollte überdacht, eine neue Lösung angeschafft werden. Tommy Grimmer, Leiter der Abteilung IT-Steuerung bei der Thüringer Aufbaubank: „Wichtig war uns, dass sie eine gute Usability mitbringt und alle jetzigen und kommenden Anforderungen der MaRisk und BAIT – soweit absehbar - erfüllt. Deshalb entschieden wir uns für die Software von Beta Systems, nicht zuletzt, weil eine Reihe anderer Banken bereits mit Garancy arbeitet und uns positive Erfahrungen berichteten."

DAS UNTERNEHMEN

Die Thüringer Aufbaubank (TAB) wurde 1992 als Anstalt des öffentlichen Rechts gegründet. Eigentümer der Thüringer Aufbaubank ist der Freistaat Thüringen. Um Thüringer Unternehmen, Kommunen oder Technologie voranzubringen, arbeitet die TAB eng mit der Thüringer Landesregierung, den Banken und Sparkassen sowie der KfW-Bankengruppe zusammen. Strikte Wettbewerbsneutralität sind für die TAB selbstverständlich. Der Freistaat Thüringen leistet zu 100 Prozent Gewähr für die Thüringer Aufbaubank. Die Rechtsaufsicht über die Bank liegt beim Thüringer Finanzministerium. Der Unternehmenshauptsitz befindet sich im S-Finanzzentrum in Erfurt. In Nordhausen, Gera, Eisenach und Suhl verfügt die TAB über regionale Kundenbetreuungen.

FACTS & FIGURES

Gründungsjahr: 1992
Beschäftigte: ~ 800
Hauptsitz: Erfurt
Vorstandsvorsitzender: Matthias Wierlacher
Vorstandsmitglied: Eckhard Hassebrock

BRANCHE

Finanzdienstleistungen / Förderbank des Freistaats Thüringen

HERAUSFORDERUNG

2016 bereits hatte die Aufbaubank im Rahmen eines IT-Governance-Projektes ein zentrales Tool zur Identitäts- und Berechtigungsverwaltung eingeführt. Nach einem Jahr Betrieb und mit Blick auf die Entwürfe der MaRisk und der BAIT wurde jedoch deutlich: Die Software würde den steigenden regulatorischen Anforderungen in der damaligen Ausprägung auf Dauer nicht genügen.

EINGESETZTE PRODUKTE

GARANCY IDENTITY MANAGER, GARANCY USER CENTER, GARANCY RECERTIFICATION CENTER

NUTZEN DER EINGESETZTEN BETA SYSTEMS LÖSUNG

Mit Garancy werden Rollen auf Fachlichkeit, Stellen und Funktionen geschnitten. Die Aufbaubank kann damit ihr Prinzip „Kein Recht ohne Rolle" umsetzen: Wer dieselbe Stellenbeschreibung hat, hat auch dieselben Zugriffsrechte und erhält dieselbe Fachrolle.

WETTBEWERBSVORTEIL

Der Einsatz des GARANCY Identity Manager automatisiert und verkürzt die Berechtigungsvergabe bei Neueinstellungen, Abgängen und sich ändernden Aufgabegebieten einzelner Beschäftigter. IT-Bereich und Führungskräfte werden dadurch von manuellen Arbeiten entlastet und können sich verstärkt auf Tätigkeiten mit Kund*innen konzentrieren.

KENNZAHLEN

Angeschlossene Systeme: rd. 65

Eingerichtete Rollen: 5.540 technische Rollen (12.700 Einzelrechte)

Verwaltete Konten: Ca. 1.100 inkl. technischer User, externe Mitarbeiter*innen

Dauer der Implementierung: Stufe 1 (03/2019-11/2019) Einführung Garancy Suite; Stufe 2 (seit 01/2020) Redesign von Benutzerberechtigungen „Rollenbau"

Rechte werden nur über Rollen beantragt

Im ersten Schritt übernahm das Projektteam 2019 alle bisher verwalteten Berechtigungen 1:1 in das neue System GARANCY Identity Manager. In der zweiten, ab 2020 startenden Stufe, beschäftigte sich die Aufbaubank mit dem Redesign der Berechtigungen. Das Grundprinzip dabei: Kein Recht ohne Rolle, d.h. Rechte werden nur über Rollen beantragt, die Vergabe von Einzelrechte erfolgt nur in Ausnahmefällen (bspw. temporäre Lese- und Schreibrechte auf Projektverzeichnisse). Mit Profilen und Rollen arbeitet die Aufbaubank schon seit langem, vor allem in der Sachbearbeitung. Die Berechtigungsgestaltung treibt also schon immer die Fachlichkeit, „aber nie so umfänglich und tiefgreifend, wie sie das Minimal- bzw. Need-to-know-Prinzip gefordert hätte", blickt Tommy Grimmer zurück. Auf Fachbereichsebene wurde also bereits geclustert, aber nicht mit dem Niveau und der Tiefe wie nun mit der neuen IAM-Lösung.

„Erst mit Beta Systems werden die Rollen wirklich auf Fachlichkeit, Stellen und Funktionen geschnitten", erklärt Cindy Schöneweck, Compliance-Referentin in der IT-Steuerung der Aufbaubank und eigens für das neue IAM-Vorhaben eingestellt. In enger Abstimmung mit der Organisationsabteilung, den Fachbereichen und der unabhängigen IT-Beraterin Dr. Claudia Walhorn, die GARANCY bereits in anderen (Investitions-)Banken mit eingeführt und begleitet hat, koordinierte sie die Einführung des IAM-Systems. Einer ihrer Grundsätze: Für jede Anwendung mit Benutzer*innenverwaltung existiert ein eigenes Berechtigungskonzept. In der Anwendung „Intranet" gibt es zum Beispiel Rechte zum Lesen, Schreiben und Administrieren. Diese werden gebündelt in sogenannte Basis,- Organisations-, Fach- oder Funktionsrollen (Rollentypen), die sich aus dem Organigramm der Bank ableiten. So haben alle Beschäftigten eine Basisrolle, die die Zeiterfassung, den Zugriff auf bestimmte Applikationen (E-Mail, AD) und Netzlaufwerke etc. regelt. Zu jeder Stellenbeschreibung gibt es außerdem eine Fachrolle, ferner Organisationsrollen für Organisationseinheiten und bereichsübergreifende Funktionsrollen (u.a. Personalrat).

In den Sachgebieten verfügen viele Beschäftigte über dieselbe Fachrolle. So sind ca. 200 Personen aus zwei großen Fachbereichen rund 21 Fachrollen zugeordnet. Diese Rollenaufteilung nimmt die Bank derzeit in GARANCY in enger Absprache mit den Fachbereichen vor und bereinigt in diesem Zuge auch bestehende Rechte.

Administrativer Aufwand bei der Rechtevergabe sinkt

Aus dem Prinzip „Kein Recht ohne Rolle" folgt also bei der Aufbaubank: Wer dieselbe Stellenbeschreibung hat, hat auch dieselben Zugriffsrechte und dem wird dieselbe Fachrolle zugewiesen. Bei jedem Neuzugang werden nun aus einem bestehenden Set an Rechten und Rollen genau die ausgewählt, die für die eigene Tätigkeit benötigt wird. Rollenbildung vereinfacht also die Zuweisung der Rechte: Alle bekommen die Basis-, Fach- und ggf. Organisations- und Funktionsrolle, die das künftige Profil im Unternehmen widerspiegelt. Dadurch sinkt der administrative Aufwand bei der Rechtevergabe deutlich. Tommy Grimmer: „Ziel ist es, aufgrund der Organisationseinheit automatisch Rollen zuzuweisen. Wenn unser HR-System SAP HCM einen neuen Beschäftigten in Organisationseinheit A mit der dazugehörigen Stellenbeschreibung meldet, erhält er automatisch die entsprechende Organisationsrolle bzw. Fachrolle zugewiesen."

„Wir sehen uns mit der aktuellen Lösung gut aufgestellt."

Tommy Grimmer

Leiter der Abteilung IT-Steuerung

„Die Berechtigungsgestaltung aus Rollen heraus, die Rollenanpassung und Pflege der Rollenkonzepte können wir mit GARANCY auf einem Niveau und in einer Tiefe betreiben, die unser voriges IAM-System nicht ermöglicht."

Cindy Schöneweck

Compliance-Referentin in der IT-Steuerung

Ableitung der Kritikalität von Rollen aus vorhandenen Informationen

„Wir mussten bei diesem IAM-Vorhaben drei verschiedene Mandanten – neben der Aufbaubank noch zwei Tochtergesellschaften – an das System anbinden", erklärt Cindy Schöneweck. Als weitere Besonderheit beschreibt sie, dass sich die Kritikalität der Rollen aus den gegebenen Informationen ableiten. Was ist damit gemeint? Zu jedem Recht muss die Frage aufgeworfen werden, wie kritisch es ist. Klassiker sind administrative Rechte, die immer kritisch sind. Auch technische User können kritisch sein. Oder es gibt kritische Rechte im Fachbereich, weil damit Zahlungstransaktionen vorgenommen werden. Anhand der Kritikalität wird auch der Rezertifizierungsturnus festgelegt, ob halbjährlich, jährlich oder alle drei Jahre.

Deshalb hat die Aufbaubank noch mit dem alten IAM-System sogenannte Informationscontainer aufgebaut. In ihnen sind ähnliche oder gleiche Daten und Informationen geclustert. Die IT weiß, welche Informationscontainer es gibt und auf welchen Systemen die Informationen verarbeitet werden.

Hier wird dann noch eine weitere Information hinzugegeben: das Mapping an Rechten in den Systemen zu den jeweiligen Containern. Dadurch kann die Kritikalität der Informationsinhalte auf die Rechte abgeleitet und somit deren Kritikalität bestimmt werden. Es lässt sich eine Schutzbedarfsfeststellung treffen, die besagt, wie hoch das notwendige Schutzniveau für eine bestimmte Information ist. Claudia Walhorn: „Durch eine solche Containerisierung kommt man gut zu der Einsicht, was auch in fachlicher Sicht ein kritisches Recht ist. Jeder Rolle wird der Informationscontainer mitgegeben und daraus leitet sich dann deren Kritikalitätsstufe ab."

4 Kernsysteme und 60 weitere Anwendungen im IAM erfassen

Nächste Schritte bei Umsetzung des IAM-Konzeptes sind die erste Rezertifizierung und der Aufbau weiterer Fach-, Funktions- und Organisationsrollen. Außerdem sollen die restlichen Anwendungen nach GARANCY übernommen werden. Wie üblich, band das Projektteam zunächst die wichtigsten Kernsysteme automatisch an die IAM-Software an.

Bei der Aufbaubank gehören hierzu SAP mit dem juristischen Datenbestand und den HCM-Daten, das Windows Active Directory sowie die zwei Eigenentwicklungen zur Sachbearbeitung von Zuschüssen und Darlehen und die „TAB-Informationssysteme", welche den größten Teil aller für Auswertungen, Berichterstattung etc. benötigten Daten der Thüringer Aufbaubank auf Einzelsatzebene und in aggregierter Form zusammenfasst. Hinzu kommt noch die Portallösung, über die die Antragsteller*innen ihre Kommunikation mit der Bank starten. Des Weiteren gibt es rund 60 Anwendungen, die halbautomatisch mit der IAM-Lösung über die uConnect Advance-Technologie von Beta Systems verknüpft werden.

Für jedes dieser Systeme braucht man aber zunächst ein eigenes Berechtigungskonzept. Cindy Schöneweck: „Wir denken derzeit auch über die Anschaffung des Garancy Role Centers nach, mit dem wir die Rollenanpassung und Pflege der Rollenkonzepte noch vereinfachen können." Im Herbst 2020 steht zunächst einmal das Update auf die aktuelle GARANCY-Version 3 an. Durch die Corona-Pandemie und die damit verbundene Antragsflut haben sich alle Vorgänge der IAM-Einführung ein wenig nach hinten verschoben.

Der guten Zusammenarbeit mit Beta Systems tat dies keinen Abbruch. „Wir schätzen an Beta Systems, dass wir hier stets feste Ansprechpartner haben und auch der Support sehr gut erreichbar ist", so Cindy Schöneweck. Nach Anschubleistung durch die externe IT-Beraterin ist sie seitdem federführend darin, die aktuellen regulatorischen Anforderungen aufzunehmen und in die Prozesse zu überführen sowie die Organisationsabteilung, Technik und Fachbereiche in allen Fragen rund um IAM zu koordinieren. Ihr vorrangiges Ziel: Die Fachbereiche müssen verinnerlichen, dass die Rechte, die sie in den Anwendungen nutzen, ihnen gehören und sie für deren Gestaltung die Verantwortung tragen.

Tommy Grimmer: „Die MaRisk-Novelle 2017 hat neue Anforderungen mit sich gebracht, die sich in bankinternen Prozessen und Abläufen niederschlagen. Und die regulatorischen Anforderungen durch die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) werden künftig kaum sinken. In der Umsetzung der Anforderungen in den eigenen Prozessen muss sich allerdings die Frage gestellt werden, wie viel mehr Sicherheit immer konkretere Anforderungen wirklich bringen und inwieweit hier das Proportionalitätsprinzip noch eingehalten wird. Wir sehen uns mit der aktuellen Lösung jedoch gut aufgestellt."

Beta Systems IAM Software AG

Alt-Moabit 90d | 10559 Berlin, Germany
+49 (0) 30 726 118 0
iam@betasystems.com
www.betasystems-iam.de