ANWENDERBERICHT: BANK FÜR SOZIALWIRTSCHAFT

Ganzheitliches Berechtigungs-management im hochsensiblen Bankwesen

Die BFS stand vor der Aufgabe, hohe regulatorische Anforderungen an die Berechtigungsvergabe kurzfristig zu erfüllen. Im Rahmen eines ambitionierten Projekts gelang die automatisierte Rezertifizierung der Benutzerberechtigungen in nur acht Monaten. Heute verfügt die BFS über eine auf SailPoint IdentityIQ basierende Software-Lösung, welche Geschäftsprozesse ebenso wie Zuständigkeiten umfassend im Berechtigungsmanagement abbildet.

Komplexe Software-Landschaft

Im Kerngeschäft zählt die BFS auf eine umfangreiche Applikationspalette. SAP-Software spielt dabei eine tragende Rolle. Derzeit befinden sich zehn SAP-Systeme im Einsatz. Alleine SAP ERP schlägt mit 19 Modulen zu Buche. Dazu gesellt sich noch eine stattliche Anzahl kleinerer Applikationen. Insgesamt verwaltet die BFS rund 700 Identitäten, von denen ein beträchtlicher Anteil auf externe Mitarbeiter entfällt, die per Citrix auf die Systeme der Bank zugreifen.

Handlungsbedarf wegen regulatorischer Vorgaben

Der Umstieg auf softwarebasiertes Identity und Access Management (IAM) ergab sich daraus, dass bei der BFS eine Reihe prozeduraler Anpassungen vorgenommen werden mussten, die eine kurzfristige Rezertifizierung der Berechtigungen ausschlossen. Insbesondere die auf Spreadsheets basierende, manuelle Methodik der Überprüfung von Berechtigungen war den regulatorischen Anforderungen nicht mehr angemessen. Zudem fehlten historische Auswertungen sowie eine zuverlässige Bewertung kritischer Berechtigungen und der daraus resultierenden Risiken.

Unterstützung durch externe Partner

Im Rahmen einer Vorstudie definierte die BFS Maßnahmen zur kurzfristigen Behebung akuter Mängel. Oberste Priorität hatte dabei die Rezertifizierung der Benutzerberechtigungen. Diese war als die erste Phase einer nachhaltigen Neuordnung des Berechtigungsmanagements vorgesehen. Dazu lancierte die BFS ein ambitioniertes, auf mehrere Jahre angelegtes IAM-Projekt. Um das Projekt im vorgesehenen Zeit- und Kostenrahmen zu stemmen, band die BFS die KOGIT GmbH und weitere erfahrene Partner mit ein.

BANK FÜR SOZIALWIRTSCHAFT

Die Bank für Sozialwirtschaft AG (BFS) konzentriert sich auf das Geschäft mit Unternehmen, Verbänden, Einrichtungen, Stiftungen und anderen Organisationen, die in den Bereichen Soziales (Senioren-, Behinderten-, Kinder- und Jugendhilfe), Gesundheit und Bildung tätig sind. Das Leistungsangebot der BFS beruht auf den drei klassischen Säulen einer Universalbank: Kreditgeschäft, Einlagen-/Wertpapiergeschäft und Zahlungsverkehr. Sie gehört zu den zehn größten Banken im Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR). Die BFS hat ihren Sitz in Köln und Berlin und betreibt 16 Geschäftsstellen.

Warum SailPoint und KOGIT?

Auf Grundlage eines detaillierten Anforderungskatalogs wurden mehrere einschlägige Software-Lösungen einem umfangreichen Auswahlverfahren unterzogen. Vier Software-Produkte standen auf der Short-List für die Endauswahl. Diese wurden der BFS durch die Software-Hersteller bzw. deren Partner präsentiert. „In einem sehr überzeugenden Auftritt hat KOGIT alle Fragen umfänglich beantwortet und die geforderte Funktionalität in SailPoint IdentityIQ schlüssig dargestellt", schildert Alexander Schwarz, Teamleiter IT-Business und Berechtigungsmanagement bei der BFS.

KOGIT übernahm den kritischen Part der schnellen Erstellung der entsprechenden Pflichtenhefte sowie die Anpassung von IdentityIQ an die bankspezifischen Bedürfnisse des Berechtigungsmanagements.

Ergänzende Plugins für die Richtlinienumsetzung

Darüber hinaus wurden zwei durch KOGIT entwickelte Plugins für SailPoint IdentityIQ installiert:

- **KOGIT SoD Matrix Plugin:** Die Trennung von Zugriffen per Segregation of Duties (SoD) ermöglicht der BFS, kritische Zugangskombinationen zu managen oder zu unterbinden. Die Funktionstrennung wird dabei übersichtlich in einer Matrix dargestellt, die auf den in SailPoint IdentityIQ definierten Policies basiert. Konflikte, Grenzfälle und erlaubte Kombinationen werden nach dem Ampelprinzip markiert und sind so für Audits optimal aufbereitet.

  „Hier wird grafisch abgebildet, welche Kombinationen erlaubt oder mitigierbar sind. Rot markierte Kombinationen werden dagegen hart abgelehnt. Das kann man schön anschaulich demonstrieren", schildert Alexander Schwarz.

- **KOGIT History Plugin:** Wie sah die Rollen- und Rechtestruktur zu verschiedenen Zeitpunkten aus? Wer sollte zu bestimmten Zeiten in Rechtegruppen sein und wer war es faktisch tatsächlich? Das Plugin beantwortet diese Fragen und stellt dafür eine intuitive Benutzeroberfläche in SailPoint IdentityIQ zur Verfügung, mit der Reports erstellt und historische Suchen auf Basis von Merkmalen, Werten sowie Datum und Zeitpunkt der Zugriffsrechte in Archiven ausgeführt werden können.

  Dazu Alexander Schwarz: „Wir können jederzeit rückblickend feststellen, welche Berechtigungen wem und zu welchem Zeitpunkt erteilt oder entzogen wurden. Der Nachweis wird über den gesamten Lifecycle sauber geführt. Bei der Jahresabschlussprüfung konnten wir entsprechende Stichproben über Eintritte und Austritte von Mitarbeitern ziehen."

Rezertifizierung: Erstes Projektziel erreicht

In der komplexen Applikationswelt der BFS war die unter enorm hohem Druck angestrebte Rezertifizierung von rund 15.000 Berechtigungszuweisungen für die priorisierten Applikationen der Bank ein kühnes Ziel. Mit ihrem Engagement und ihrem Können trugen erfahrene KOGIT Consultants entscheidend dazu bei, dass dieses Ziel kurzfristig und mit erstklassigem Ergebnis erreicht wurde. „Dr. Martin Dehn von KOGIT und sein Team haben unsere bankfachlichen Anforderungen in ein ausgeklügeltes technisches Konzept übersetzt und das Projekt sehr clever und schnell realisiert", so Alexander Schwarz.

„Die Rezertifizierung der Benutzerberechtigungen war die erste und dringlichste Phase unseres IAM-Projekts. Hierfür galt ein extrem sportlicher Abschlusstermin. Externe Experten meinten, wir müssten für die gesamte Neuordnung des Berechtigungsmanagements drei bis vier Jahre ansetzen. Wir hatten aber nur 18 Monate."

ALEXANDER SCHWARZ
Teamleiter IT-Business und Berechtigungsmanagement, Bank für Sozialwirtschaft AG

Erfolgsfaktor Kommunikation

Die Einführung des Berechtigungsmanagements auf SailPoint-Basis wurde durch eine Kommunikationskampagne sowie durch Schulungen und Workshops seitens der Management Beratung Horváth & Partner umfassend begleitet. „Wir haben die aufsichtsrechtliche Vorgabe, die Verantwortung für die Berechtigungen in die Fachabteilungen hineinzutragen. Dazu müssen wir die Verantwortlichen an der richtigen Stelle abholen. Das erfordert natürlich viel Kommunikation, denn mit jedem Fachbereich muss geklärt werden, ob die Berechtigungsstrukturen für die dort genutzten Applikationen sinnvoll sind“, so Schwarz. „Erst dann kann man die entsprechenden Prozesse konzipieren und über Software sauber umsetzen, um den großen Umfang zu bewältigen.“

„Aus meiner Perspektive war der Umstieg eine ganz große Leistung. Die Fachbereiche mussten aufgrund der aufsichtsrechtlichen Anforderungen viele zusätzliche Aufgaben übernehmen. Wir haben hier ein positives Bild und Akzeptanz erreicht.“

ALEXANDER SCHWARZ
Teamleiter IT-Business und Berechtigungsmanagement, Bank für Sozialwirtschaft AG

Planmäßiger IAM-Ausbau

Mit der erfolgreichen Rezertifizierung der Benutzerberechtigungen hat die BFS die erste große Hürde in Richtung nachhaltige Compliance genommen. Ein wesentlicher Faktor war hierbei die hohe Motivation und Lernbereitschaft bei den BFS-Kollegen sowie die nahtlose Zusammenarbeit der externen Projektpartner. KOGIT übernahm hierbei die technische Konzeption und Umsetzung des Projektes, Horváth und Partners waren verantwortlich für das Projektmanagement sowie die inhaltlichen Klärungen mit den Fachbereichen.

In der nächsten Ausbaustufe wird die BFS die Zugriffsberechtigungen auf die Daten und Anwendungen der Bank effizienter, transparenter und revisionssicher verwalten können. Die durch KOGIT implementierte Lösung schafft hierfür klare und sicher beherrschbare Strukturen im Berechtigungsmanagement, automatisiert die gesetzlich geforderte Nachweisführung und trägt wesentlich zur Früherkennung von Zugriffsrisiken bei.

Derzeit bindet das Berechtigungsmanagement-Team der BFS weitere berechtigungsrelevante Applikationen und Prozesse sowie Windows Ressourcen in SailPoint IdentityIQ ein. Alexander Schwarz betont, dass die Abbildung der regulatorischen Anforderungen nur mittels Automatismen vernünftig darstellbar ist. Als Beispiel nennt er die automatische Auspflege austretender Benutzer mit entsprechendem Berechtigungsentzug. Der Wartungs- und Pflegeaufwand verringert sich dadurch immens.

Auch bei der aktuell laufenden Anbindung von Windows Active Directory-Ressourcen leistet KOGIT wertvolle Konzeptions- und Implementierungsarbeit.

Support durch KOGIT

Neben dem Wartungsvertrag für SailPoint IdentityIQ hat die BFS auch einen Solution Supportvertrag mit KOGIT abgeschlossen. „Das System ist noch recht jung und erfordert auch beim weiteren Ausbau Customizing. Deshalb richten wir regelmäßig Supportanfragen an KOGIT. Wir haben dafür einen Hauptansprechpartner, der uns gut bedient. Mit der Erreichbarkeit und der geleisteten Unterstützung sind wir sehr zufrieden“, resümiert Alexander Schwarz.

Das Projekt im Überblick

Zielsetzung

- Kurzfristige Rezertifizierung der Benutzerberechtigungen nach BaFin-Vorgabe
- Nachhaltige Erfüllung grundlegender Compliance-Anforderungen für die Kernsysteme
- Automatische Verwaltung zahlreicher, online angebundener Zielsysteme (z.B. SAP)
- Automatisierte Berechtigungsvergabe
- Bestellprozess mit einfacher und doppelter Freigabe

Lösung

- Einführung von SailPoint IdentityIQ als Software-Plattform für das Berechtigungsmanagement
- Funktionalitätserweiterung durch Plugins für die organisatorische Funktionstrennung und das Tracking der Berechtigungshistorie Überarbeitung der SAP-Systeme mit Blick auf Risikominimierung
- Verlagerung der Verantwortlichkeiten für die Berechtigungen in die Fachabteilungen

Ergebnisse

- Fristgerechte, automatisierte Rezertifizierung der Benutzer-berechtigungen auf den wichtigsten Systemen
- Erweiterung, Ausbau und Optimierung des Berechtigungs-managements hin zu einer ganzheitlichen IAM-Lösung für nachhaltige Compliance
- Deutliche Reduzierung der manuellen Administration von Zielsystemen

PARTNERSCHAFT KOGIT & SAILPOINT

KOGIT war der erste europäische SailPoint-Partner. Als einziger deutscher Partner gehört KOGIT dem SailPoint Partner Advisory Board an und ist Mitglied der Identity+ Alliance. Mit 45 Mitarbeiter – davon 35 SailPoint Berater – ist KOGIT der Partner mit dem größten SailPoint-Kompetenzteam in Europa. Nach der Auszeichnung als „Partner of the Year Europe 2015“ wurde KOGIT 2018 als einziger deutscher Partner von SailPoint zum Top16 Delivery Admiral 2018 ernannt.

KONTAKT

KOGIT GmbH
Rheinstr. 40-42
64283 Darmstadt

Telefon: +49 6151 7869-0
info@kogit.de · www.kogit.de