_Kunde & Anforderung

Zahlreiche Mängel im Berechtigungsmanagement

Der Kunde – ein großer deutscher Bankkonzern mit ca. 8.000 Mitarbeitern – ist insbesondere in den letzten Jahren durch Ausbau seines Kerngeschäftes und Unternehmenszukäufe stark gewachsen. Gleichermaßen haben die aufsichtsrechtlichen Anforderungen an die IT deutlich zugenommen.

Für die Verwaltung von Zugriffsrechten für Mitarbeiter auf Systeme der Bank setzt der Kunde ein zentrales „Identity & Access Management System" ein. Aufgrund der historischen Weiterentwicklung der Anwendungslandschaft ergeben sich in Teilen intransparente Strukturen in einzelnen Berechtigungen für Endanwender.

MaRisk AT 7.2 Technisch Organisatorische Ausstattung
„[...] Prozesse für eine angemessene IT-Berechtigungsvergabe [sind] einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt […]"

(„Minimalprinzip" oder „Need-to-Know Prinzip")

Vor diesem Hintergrund konnte nicht festgestellt werden, über welche **zulässigen Rechte** ein Mitarbeiter der Bank verfügt. Tendenziell wurden Mitarbeitern deutlich mehr Rechte eingeräumt oder bei internem Wechsel weitervererbt, ohne dass sie diese für deren tägliche Arbeit benötigten. Aufgrund dessen konnten mögliche **Interessenskonflikte nicht ausgeschlossen** werden.

Interne Kontrollen waren teilweise nicht wirksam, da die Transparenz über die Rechte sowie deren Beschreibung unvollständig waren. Somit konnten Führungskräfte der Bank ihre Verantwortung in der Rechtevergabe nicht vollständig wahrnehmen.

Feststellungen aus internen und externen Prüfungen erforderten zwingend Handlungsmaßnahmen, um strukturelle Mängel im Berechtigungsmanagement zu beheben.

_Zielsetzung

Einführung eines Rollenmodells und risikoorientierte Bereinigungsmaßnahmen

Als Grundlage wirksamer Vergabe- und Kontrollprozesse ist eine **vollständige Dokumentation der zulässigen Rechte** für Endanwender und privilegierte Nutzer erforderlich.

Gleichzeitig sind derzeit vergebene **Rechte zu überprüfen** und nach einem fachlichen Schnitt **in Rollen zu bündeln**. Bankweit ist ein Rollenmodell zu etablieren, um Rechte nachvollziehbar an Anwender zu vergeben.

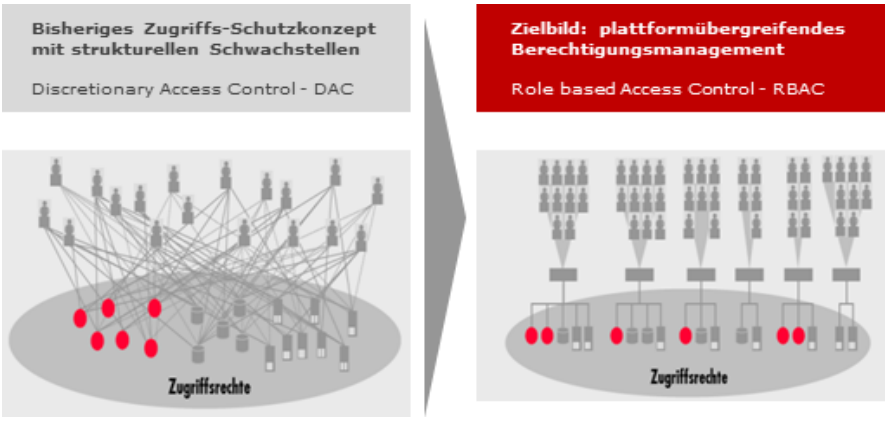


Abbildung: Vergleich Zugriffsrechte vorher und nachher (Quelle: Eigene Darstellung)

Die Zugriffsrechte für Systeme und Datenbanken sind zu überarbeiten. Die Anzahl von **kritischen Rechten** ist auf ein erforderliches Mindestmaß einzuschränken und durch geeignete Sicherungsmaßnahmen und Kontrollen zu überwachen.

_Vorgehensweise

Einbindung der IT und Fachbereiche als wesentlicher Erfolgsfaktor

Für die Überprüfung, Neustrukturierung und Dokumentation der Zugriffsrechte sind technische wie auch fachliche Kenntnisse gleichermaßen erforderlich. Somit ist die Unterstützung der Applikationsverantwortlichen innerhalb der IT und der Fachbereiche ein wesentlicher Erfolgsfaktor. Um eine effektive bankweite Kommunikation aufrechtzuerhalten, wurde hierzu eine Kommunikations-plattform etabliert.

Von prozessualen Anpassungen bis hin zur Entwicklung und Umsetzung eines rollenbasierten Berechtigungsmanagement wurden alle Maßnahmen zentral gesteuert, um eine enge Synchronisation der einzelnen Tätigkeiten zu erreichen. Abhängigkeiten bspw. in der Dokumentation und Bereinigung von Rechtestrukturen konnten dabei berücksichtigt werden sowie möglichen Risiken bspw. in der Arbeitsfähigkeit von Mitarbeitern durch Rechteentzug entgegengewirkt werden.

Bei allen Maßnahmen steht die nachhaltige Ausgestaltung des Berechtigungsmanagements der Bank im Vordergrund, um einen aufsichtsrechtlich-konformen wie auch wirksamen Regelbetrieb langfristig zu gewährleisten.

_Leistungen

Stringentes Projektmanagement und fachliche Expertise gefordert

Für eine erfolgreiche und zeitgerechte Umsetzung konnten bewährte methodische Verfahren und fachliche Erfahrungen eingebracht werden. Severn unterstützte insbesondere bei:

- Definition und **Nachverfolgung von geeigneten Maßnahmen** zur nachhaltigen Behebung der strukturellen Mängel im Berechtigungsmanagement
- Methodische **Qualitätssicherung** und Prüfung von Vorgehensweisen anhand bewährter Marktstandards und –verfahren
- Organisation von Workshops, Schulungen, Etablierung eines „Arbeitsmodells" zwischen IT und Fachbereichen
- Review und Optimierung der Prozesse und Kontrollen im Berechtigungsmanagement
- Adressatengerechte **Kommunikation** zu internen Stakeholdern, Senior Management und internen wie externen Prüfern sowie Aufsicht
- **Coaching** von Teilprojektleitern und Managern in der effektiven Umsetzung von Maßnahmen
- Revisionskonforme Aufbereitung der Ergebnisse

_Ergebnisse und Kundennutzen

Nachhaltige Verankerung

Mittels einer vollständigen Dokumentation der Berechtigungskonzepte und einem transparenten Rollenmodell ist es künftig nachvollziehbar, welche Rechte für welche Mitarbeiter zulässig sind.

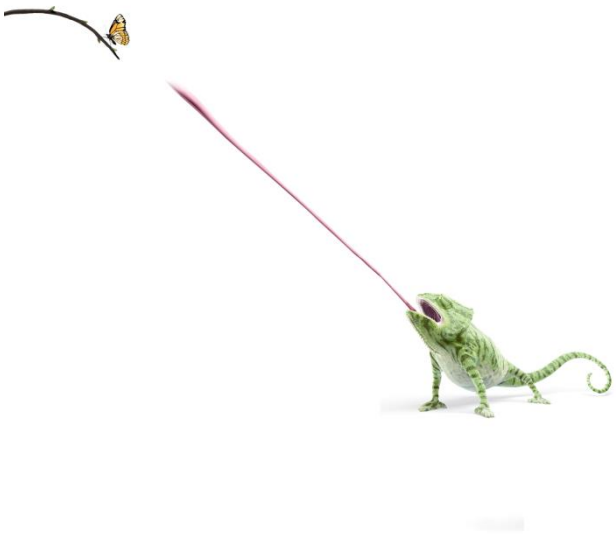
Mit der Prüfung und Bereinigung der Zugriffsrechte wurde die bestehende Rechtesituation auf das dokumentierte Zielbild angepasst, nicht benötigte Rechte entzogen und unzulässige Rechtekombinationen aufgelöst.

Bestehende Feststellungen wurden fristgerecht behoben und durch überarbeitete Prozesse in der Rechtevergabe und -kontrolle die Wirksamkeit des Berechtigungsmanagements des Kunden erhöht. Damit werden nicht allein regulatorische Anforderungen erfüllt; auch das interne Sicherheitsniveau wurde deutlich verbessert. Mitarbeiter verfügen nunmehr nachvollziehbar über die Rechte, die sie für ihre Tätigkeit benötigen.

_Ihr Partner

Severn Consultancy

Next Generation Consulting
für Finanzunternehmen



_Ansprechpartner:

Norman Nehls | Partner

Severn Consultancy GmbH
Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
T +49 (0)69 / 950 900-0
F +49 (0)69 / 950 900-50
info@severn.de
www.severn.de