IT-RECHTE-VERGABE BEI BANKEN

Methodischer Vier-Punkte-Ansatz zur sicheren und effizienten Verwaltung von IT-Berechtigungen

Banken wickeln ihre Geschäfte zu 90 Prozent IT-basiert ab. Daher ist für sie eine lückenlose IT-Security unabdingbar. Eingefordert wird dabei vor allem die Transparenz bei existierenden Berechtigungen und die Nachvollziehbarkeit bei den Prozessen der Berechtigungsvergabe. Die Münchner econet GmbH, ein führender Anbieter von prozessorientierter Unternehmenssoftware für das Identity und Access Management, hat vier Top Tipps auf Basis seiner Lösung econet Identity & Service Manager zusammengestellt. Damit optimieren Banken ihr Risikomanagement und ihre Compliance-Erfüllung auf dem Gebiet der unternehmensweiten Berechtigungsverwaltung.

Ein zentraler Punkt fast aller hierfür geltenden Standards und Gesetze impliziert die Frage: Wer darf was in den IT-Systemen? Sowohl die Transparenz bei den existierenden Berechtigungen als auch die Nachvollziehbarkeit bei den Prozessen der Berechtigungsvergabe muss gewährleistet werden. Theoretisch einfach, praktisch schwierig: Banken sind fleißige Fusionierer und Umorganisierer und oft müssen fremde IT-Landschaften integriert und an bestehende Prozesse angepasst werden. Darum sehen die IT-Strukturen und Prozesse in Wirklichkeit eher chaotisch als geordnet aus. Besonders bei den Rechtestrukturen in Dateisystemen, die aufgrund fehlender Management-Tools kaum beherrschbar wuchern. Da zudem der Beruf „Bankkaufmann“ ein Ausbildungsberuf ist, ist es unabdingbar, beim Gang durch die einzelnen Abteilungen sichere Provisionierungs- und vor allem De-Provisionierungs-Prozesse zu haben, um IT-Berechtigungen regelkonform gewähren und entziehen zu können.

Um den bankenspezifischen Forderungen wie MaRisk oder KonTraG gerecht zu werden, ist es außerdem wichtig, dass Berechtigungen über Genehmigungsverfahren mit „Vier-Augen-Prinzip“ eingehalten vergeben werden, um jederzeit Auskunft darüber geben zu können, wer welche Rechte genehmigt hat. Doch wie können die geforderten Genehmigungs- und Kontrollverfahren in bestehenden, gewachsenen IT-Strukturen einfach und sicher etabliert werden?

econet hat hierfür einen methodischen Ansatz in vier Schritten entwickelt, der sowohl die Analyse bestehender Berechtigungen und möglicher Schwachstellen in Dateisystemen als auch die Prävention von Risiken durch ein Identitätsmanagement mit geregelter Rechtevergabe garantiert:

Schritt 1
Im ersten Schritt werden die Berechtigungen, die sich über Jahre in den gewachsenen Dateisystemen angesammelt haben, automatisiert ausgelesen Die Berechtigungsdaten können dann zu Revisions- und Risikomanagementzwecken zur Verfügung gestellt werden. Ein Beispiel hierfür sind Audits nach dem Standard SSAE 16 (früher SAS-70) im Rahmen der Bewertung von SOX-Compliance.

Auch im internen Security-Assessment identifiziert eine Audit-Lösung wie das Reporting Studio von econet mögliche Risiken. Dabei wird nicht nur der Risikograd der gefundenen Schwachstellen bewertet, sondern auch eine Einschätzung zum Aufwand ihrer Behebung in Form von Kennzahlen gegeben. So lässt sich praktisch auf Knopfdruck eine faktenbasierte Priorisierung für die meist sehr zeitintensiven „Sicherheitsreparaturen“ aufstellen.

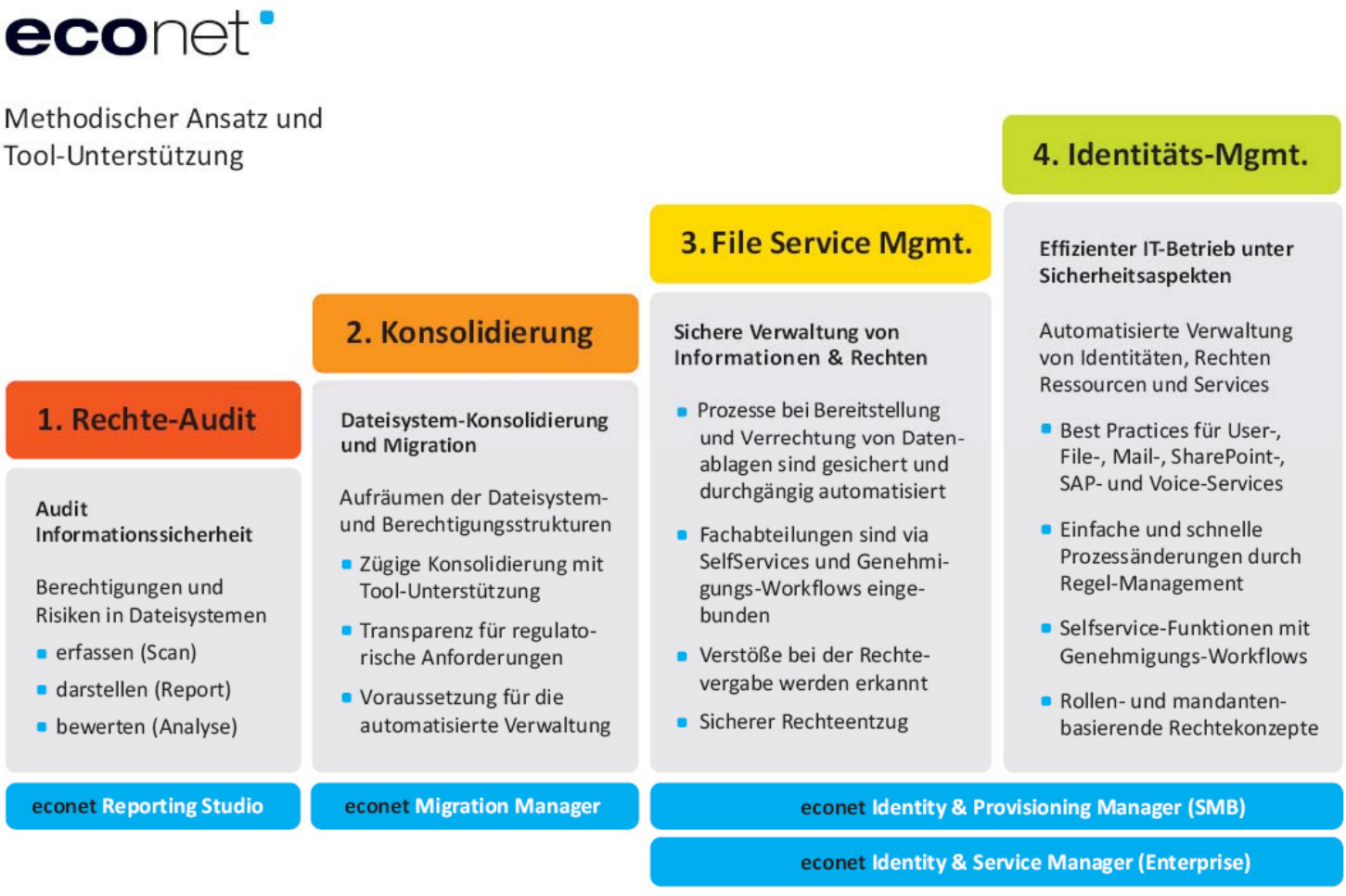
Schritt 2
Im zweiten Schritt muss eine einheitliche Struktur des Dateisystems geschaffen werden. Das heißt: Die wild gewachsenen Dateisystemstrukturen müssen so beschaffen sein, dass eine zentrale und weitgehend automatisierte Verwaltung der Berechtigungen darauf möglich wird. Abhilfe schaffen passende File-Service-Konzepte, nach deren Vorgaben die herkömmliche Dateisystemverwaltung in ein sicher provisioniertes Dateisystem überführt werden kann, ohne die Konsistenz in den Geschäftsprozessen oder die Datensicherheit zu beeinträchtigen.

Schritt 3
Auf Basis eines einheitlichen File-Service-Konzepts kann nun ein FS-Management toolgestützt eingeführt werden, das rechtliche Anforderungen in besonderer Weise berücksichtigt und erfüllt. Zum einen sind dies automatisierte Prozesse für die Rechtevergabe und den Rechteentzug, die durchgängig sind und deren Umgehung nicht unentdeckt bleibt. Zum anderen geht es um Genehmigungsverfahren mit der Entscheidung in den Fachabteilungen. Dabei werden nur den wirklich autorisierten Anwendern Zugriffsrechte auf Informationen gewährt – also einheitliche, effiziente und Compliance-konforme Prozesse nach dem Vier-Augen-Prinzip.

Schritt 4

Der letzte Schritt zum zentralen Management von Identitäten und Rechten ist der automatisierte Import der User-Daten in ein Identitäts-Management-System. Nach dem Definieren von organisatorischen Rollen können nun weitere Genehmigungs-Workflows implementiert werden. Ab jetzt können beispielsweise beim Weggang von Mitarbeitern deren kompletten Berechtigungen von zentraler Stelle aus zuverlässig gesperrt oder neue Mitarbeiter in den Systemen angelegt werden - automatisiert und mit exakt den Berechtigungen, die sie für ihre Arbeit benötigen.

„Durch den Einsatz der econet-Lösung werden die wichtigsten Prozesse bei der Vergabe von IT-Rechten in Banken sicherer und effizienter abgewickelt. Vor allem die unüberschaubaren De-Provisioning-Prozesse lassen sich nun von zentraler Stelle aus automatisiert durchführen“, erläutert Thomas Reeb, Leiter Vertrieb und Marketing der econet GmbH. „Mit diesem Ansatz können Banken die geforderten Genehmigungs- und Kontrollverfahren in IT-Strukturen einfach und sicher integrieren.“



Weitere Informationen finden Sie unter www.econet.de.

Über econet

Die econet GmbH ist ein führender Anbieter von prozess-orientierter Software in den Bereichen Identity Management und Service Management mit Kernkompetenzen in Data Provisioning, File Service Management und bei der Berechtigungs-Analyse. Seit 1994 steht econet dem gehobenen Mittelstand ebenso wie Dax-Unternehmen oder großen Behörden beim Betrieb und der Absicherung ihrer Kern-IT-Dienste zur Seite.

econet bietet einen methodischen Ansatz zum schrittweisen Aufbau geeigneter Maßnahmen
- um wachsenden Compliance-Anforderungen schnell und mit vertretbarem Aufwand nachzukommen
- um mit der Automatisierung von Prozessen einen sicheren und effizienten IT-Betrieb zu gewährleisten
- um den Bezug von IT-Diensten wie Anwendungen, E-Mail oder Dateiablagen so einfach und transparent zu gestalten, wie das Bestellen eines Buchs im Online-Shop