

Vier-Punkte-Ansatz: Verwaltung von IT-Rechten

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, ein Anbieter von prozessorientierter Unternehmenssoftware für das Identity- und Service-Management, hat daher vier Toptipps auf Basis seiner Lösung cMatrix zusammengestellt. Damit optimieren Banken ihr Risiko-Management und ihre Compliance-Erfüllung bei der unternehmensweiten Berechtigungsverwaltung. Ein zentraler Punkt fast aller Regularien 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.

Um den bankenspezifischen Forderungen wie 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**

Zuerst 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 ist ein SAS-70-Bericht im Rahmen der Bewertung von SOX-Compliance.

→ **Schritt 2**

Im zweiten Schritt ist eine einheitliche Struktur des Dateisystems zu schaffen. 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 Fileservice(FS)-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 Fileservice-Konzepts kann nun ein FS-Management toolgestützt eingeführt werden, das rechtliche Anforderungen in besonderer Weise berücksichtigt und erfüllt. 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 Identity-Accessmanagement-System. Nach dem Definieren von organisatorischen Rollen können nun weitere Genehmigungsworkflows implementiert werden. Ab jetzt können beispielsweise beim Weggang von Mitarbeitern deren Berechtigungen von zentraler Stelle aus zuverlässig gesperrt oder neue Mitarbeiter in den Systemen angelegt werden.

www.econet.de
