

Genehmigungs- und Kontrollverfahren in bestehende IT-Strukturen integrieren

## Banken haben keinen Kredit bei IT-Rechten

Banken arbeiten in erster Linie mit dem Geld anderer Leute. Darum gelten für sie ganz besondere Regeln und Vorschriften. Neben den üblichen Datenschutzgesetzen (BDSG), Wirtschaftsprüfungsgesetzen (GDPdU), Aktiengesetzen, und SOX gibt es Gesetzgebungen, die speziell die Kreditvergabe (BASEL II) sowie die Kontrolle und Transparenz im Unternehmensbereich (KonTraG) regeln. Gemäß KonTraG ist ein Unternehmen unter anderem zum IT-Risiko-Management und zur Schaffung sicherer Netzwerkinfrastrukturen verpflichtet. Daraus leiten sich strikte Maßnahmen zur Absicherung der IT-Infrastruktur hinsichtlich Audits (lückenloser Kontrolle) und Nachweispflichten über Berechtigungsstrukturen ab. Eine unabhängige Kontrollbehörde wacht über die Einhaltung dieser Gesetzgebungen: die Bundesanstalt für Finanzdienstleistungsaufsicht oder kurz BaFin. Stellt sie Regelverstöße fest, drohen Strafen bis hin zum Verlust der Banklizenz.

Pressewirksame Vorfälle haben das Thema einer breiten Öffentlichkeit sichtbar gemacht. Etwa 1995, als der Derivatehändler

Nick Leeson durch eine Reihe von Fehlspekulationen die Barings Bank in den Ruin trieb. Dabei ging es letztlich immer um ei-

nen Rechtemissbrauch bei hochspekulativen Geschäften mit verheerenden Folgen für die Bank und ihre Kunden.

### Das Problem:

Da Banken ihre Geschäfte zu 90 Prozent über IT abwickeln, hat IT-Security einen sehr hohen Stellenwert. Ein zentraler Punkt fast aller Regulatorien und Gesetze impliziert die Frage: Wer darf was in den IT-Systemen? Eingefordert wird sowohl die Transparenz bei den existierenden Berechtigungen als auch die Nachvollziehbarkeit bei den Prozessen der Berechtigungsvergabe. Das ist leichter gesagt als getan, denn Banken sind fleißige Fusionierer und Umorganisierer und oft müssen fremde IT-Land-



