

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.

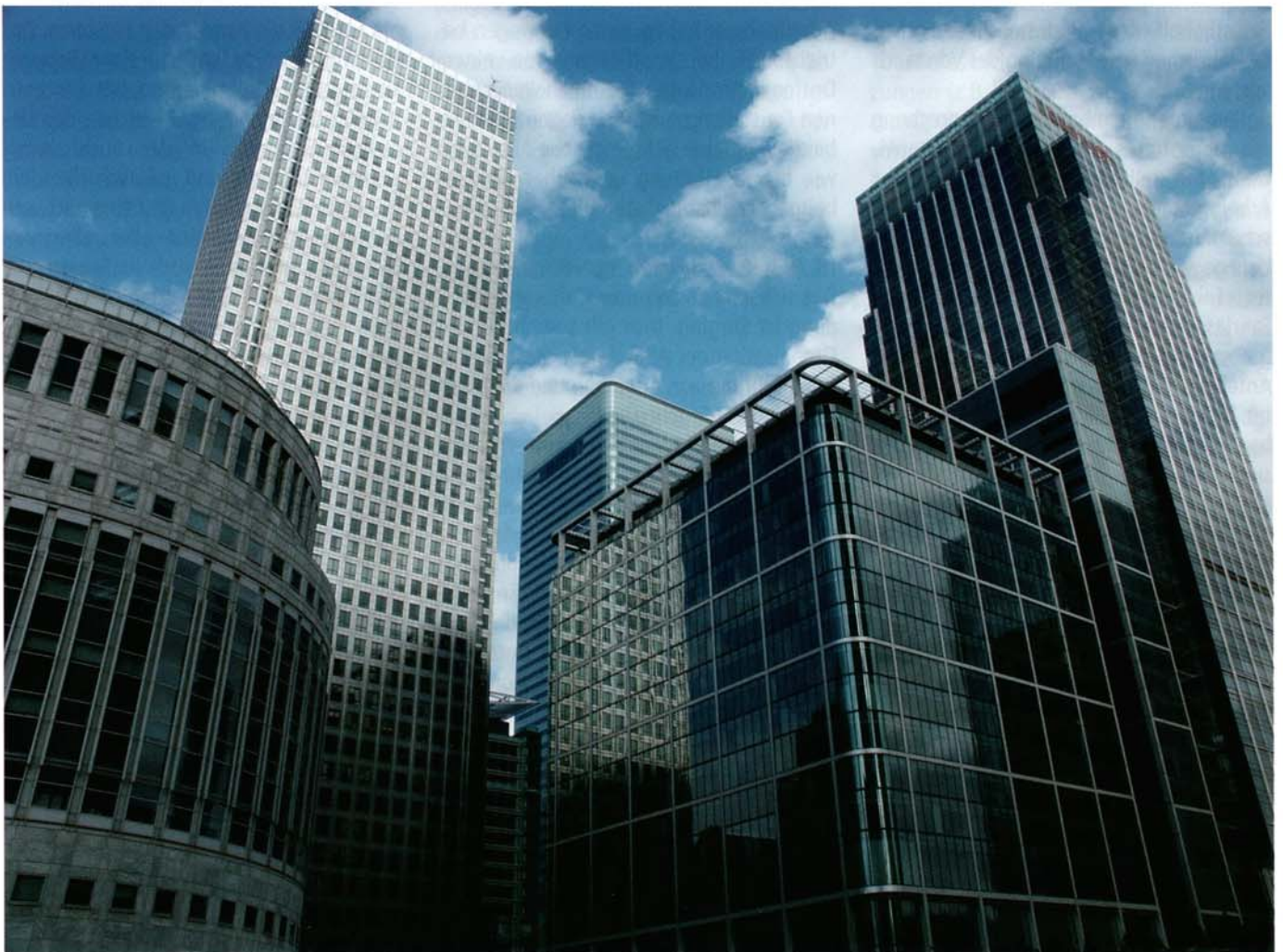
Pressewirksame Vorfälle haben das Thema einer breiten Öffentlichkeit sichtbar gemacht. Etwa 1995, als der Derivatehändler

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 Regularien 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-



schaften integriert und an bestehende Prozesse angepasst werden. Darum sehen die IT-Strukturen und -Prozesse in Wirklichkeit eher chaotisch als geordnet aus. Vor allem bei den Rechtestrukturen in Dateisystemen, die auf Grund fehlender Management-Tools kaum beherrschbar wuchern. Da zudem der Beruf „Bankkaufmann“ ein Ausbildungsberuf ist, ist es besonders wichtig, beim Gang durch die einzelnen Abteilungen sichere Provisionierungs- und vor allem Deprovisionierungs-Prozesse zu haben, um IT-Berechtigungen regelkonform gewähren und entziehen zu können. Vor allem wenn die Forderungen von KonTraG gelebt werden sollen, müssen zwingend „Vier-Augen-Prozesse“ vorgehalten werden, um jederzeit Auskunft darüber geben zu können, wer Rechte auf welche Applikationen, Fachverfahren und vertrauliche Bank- und Kundendaten hat und wer sie genehmigt hat. Doch wie können die geforderten Genehmigungs- und Kontrollverfahren in bestehenden, gewachsenen IT-Strukturen einfach und sicher etabliert werden?

#### Die Lösung:

Um diese Aufgabe zu bewältigen, wurde ein methodischer Ansatz in vier Schritten entwickelt. Er reicht von der Analyse bestehender Berechtigungen und möglicher Schwachstellen in Dateisystemen bis zur Prävention von Risiken durch ein Identitäts-Management mit Vier-Augen-Prinzip. Auf diese Weise ist eine geregelte Rechtevergabe garantiert.

#### Schritt 1

Im ersten Schritt werden die Berechtigungen, die sich über die Jahre in den gewachsenen Dateisystemen angesammelt haben, ausgelesen und konsolidiert. Da es durchaus mehrere Millionen Berechtigungen in einem Dateisystem sein können, ist mit Handarbeit hier längst nichts mehr auszurichten. Die Berechtigungsdaten können dann zu Revisions- und Risikomanagementzwecken zur Verfügung gestellt werden, beispielsweise über einem SAS-70-Bericht im Rahmen der Bewertung von SOX-Compliance.

Aber auch im internen Security-Assessment lassen sich Risiken mit einer geeigneten Analyse-Lösung identifizieren und bewerten. Eine Reporting-Lösung bewertet dabei nicht nur den Risiko-Grad der gefundenen

Schwachstellen, sondern liefert auch Einschätzungen zum Aufwand ihrer Behebung in Form von Kennzahlen. So lässt sich praktisch auf Knopfdruck eine faktenbasierte Priorisierung für die doch meist zeitintensiven „Sicherheits-Reparaturen“ aufstellen.

Mit solch einer Analyse-Lösung können auch historische Abläufe mit dem Ziel der Nachweisbarkeit rechtskonformer Berechtigungen über längere Zeiträume hinweg erstellt werden.

#### Schritt 2

Allerdings sollte das Ziel nicht das „Hinterherarbeiten“ in einem risikofälligen System sein. Höchste Priorität müssen vielmehr die Prävention von Sicherheitsrisiken und die Vorbeugung von Compliance-Verstößen haben. Das bedeutet, zuerst müssen die wild gewachsenen Strukturen von Dateisystemen so organisiert werden, dass eine zentrale und weitgehend automatisierte Verwaltung der Berechtigungen darauf möglich wird. Für diesen Zweck gibt es passende Fileservice-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 Fileservice-Management Tool-gestützt eingeführt werden, das rechtliche Anforderungen in besonderer Weise berücksichtigt und erfüllt: Zum einen sind dies durchgängig rechtskonform automatisierte Prozesse für die Rechtevergabe, 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, d.h. 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 Access Management System (IAM). Nach der Definition von organisatorischen Rollen können nun weitere Geneh-

migungswflows 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 – automatisiert und mit exakt den Berechtigungen, die sie für ihre Arbeit benötigen.

Durch den konsequenten Einsatz von Rechte-Management in einem IAM-System werden alle nötigen Prozesse bei der Vergabe von IT-Rechten sicher und effizient abgewickelt. Vor allem die unüberschaubaren Deprovisioning-Prozesse lassen sich dann von zentraler Stelle aus automatisiert durchführen.

#### Autor



**Thomas Reeb**  
Vorstand der econet AG