

Identity & Provisioning Management (IPM) und Compliance

IT-Sicherheit im Fokus von Sox, Basel II und KonTraG



Die Bedeutung von Compliance nimmt in Unternehmen stetig zu, u.a. weil inzwischen auch das Management für die Einhaltung von gesetzlichen Regelungen und Bestimmungen haftbar gemacht werden kann. Weltweit werden derzeit unter diesem Schlagwort Anforderungen diskutiert, die zahlreiche Gesetze und Standards wie SOX (Sarbanes-Oxley Act), Basel II oder der 8. EU-Richtlinie an das Risiko-Management eines Unternehmens stellen.

Da unternehmensweites Risiko-Management immer auch das IT-Risiko-Management umfasst, steht das Thema Compliance weit oben auf der IT-Agenda von Unternehmen. Das bedeutet vor allen Dingen, dass die Vergabe und Änderung von Zugriffsrechten revisionssicher dokumentiert ist und dass diese zur Risikoanalyse stets verfügbar sind. Eine Nichteinhaltung dieser Minimalforderungen, die aus allen Standards ableitbar sind, führt zunehmend zu Nachteilen wie z.B. Herabsetzung im Rahmen von Bonitätsprüfungen.

Nun stellt sich dem CIO eines Unternehmens häufig die Frage, wie er die Forderung nach Revisionierbarkeit der Zugriffsrechte erreichen kann. Als Lösung kommt hier nur eine unternehmensweite Lösung in Betracht, die sowohl die Vergabeprozesse als auch die aktuellen und historischen Berechtigungen abbilden kann. Ziel ist hier häufig die Übersicht über die aktuellen Berechtigungen im Unternehmen. Durch eine gut konzipierte IPM Lösung ist es möglich, die Berechtigungen sowohl zentral als auch dezentral zu vergeben und zu monitoren. Ohne eine derartige Lösung ist eine Übersicht nur mit akribisch geführten Listen und dem zugehörigen Aufwand möglich. Der einfache Einsatz einer IPM-Lösung schafft hier aber leider bzgl. des Gesamtproblems nur wenig Abhilfe: Um eine brauchbare Risikoanalyse durchzuführen, muss der Auditor nun die User einzeln betrachten und kann nur sehr schwierig kritische Pfade erkennen oder eine Gesamtbetrachtung des Unternehmens durchführen.

Welches sind nun die Anforderungen an eine IPM-Lösung, damit diese auch tatsächlich die Compliance verbessert? Hier sind vor allen Dingen zwei Punkte zu nennen: Einerseits muss ein leistungsfähiges Rollenkonzept vorliegen und andererseits muss eine umfassende Workflowunterstützung implementiert sein.

Das Rollenkonzept hat deswegen eine so große Bedeutung, weil die zentrale Verwaltung von Identitäten zwar eine Grundlage ist, um ein unternehmensweites Berechtigungsreporting zu ermöglichen, aber die tatsächliche Durchführung damit noch nicht gesichert ist. Der Auditor wird kaum zeitlich in der Lage sein, jeden User eines Unternehmens einzeln zu analysieren. Nur über ein ausgefeiltes Rollenkonzept, welches auch durch die IPM-Lösung unterstützt wird ist ein nutzbares Reporting realisierbar, wie das Scheitern einiger halbherzig erstellter und unterstützter IPM-Projekte aufzeigt. Dafür ist es zwingend notwendig, dass die Analyse der zu implementierenden Rollen zeitlich gestrafft durchführbar ist. Dieses kann ermöglicht werden, indem entweder die Rollen Top-Down organisatorisch ermittelt werden oder Bottom-Up eine Analyse der bestehenden Rollen als Grundlage genutzt wird. Der Charme des zweiten Ansatzes liegt darin, dass man ohne langwierige Abstimmungsrunden bestehende Berechtigungen weitestgehend zu Rollen zusammenfassen kann und somit deutlich zügiger zur Einführung eines Rollenmodells kommt. Dieser Analyseansatz wurde im Rahmen eines wissenschaftlichen Projektes durch das Institut für System-Management entwickelt und wird durch die Software „bi-cube[®] Professional“ umfassend unterstützt.

Die zweite wesentliche Voraussetzung, um die Compliance im Berechtigungsmanagement sicherzustellen, ist die Workflowunterstützung der IPM-Software. Dabei sollten insbesondere Genehmigungsschritte im Rahmen eines Antragsverfahrens die Zuweisung von Berechtigungen legalisieren und automatische Berechtigungsvergaben einen Großteil der Prozesse automatisieren. Ein idealerweise webbasiertes

Identity & Provisioning Management (IPM) und Compliance

IT-Sicherheit im Fokus von Sox, Basel II und KonTraG



Genehmigungsverfahren ermöglicht dem Auditor festzustellen, auf Grund wessen Autorisierung ein Mitarbeiter ein Recht zugewiesen bekommen hat. Auf der anderen Seite können Prozessautomatisierungen einen Großteil der Fehler ausschließen und die Standardprozesse für den Audit deutlich vereinfachen.

Das Zusammenspiel von Rollen, Antragsverfahren und Workflow im Rahmen eines IPM stellt eine Toolbox dar, die die Revisionssicherheit bzgl. der Berechtigungen in der Praxis erst ermöglicht, da auf diese Weise die Gesamtheit der Berechtigungen und kritische Pfade auch tatsächlich ermittelbar sind.

