

# Darf der das?

## Schwachpunkt Berechtigungsmanagement

Autor: Stephan Brack, Geschäftsführer protected-networks.com GmbH

**Viele Unternehmen schützen ihre IT-Systeme vor allem vor Angriffen von Außen. Doch interne Schwachstellen, die durch zu liberale und unkontrollierte Rechtevergabe entstehen, finden noch zu wenig Beachtung.**



Nicht für jeden freigegeben: Zugangsrechte müssen verwaltet werden. Quelle: iStockphoto/ricardoinfante

Bei internem Datendiebstahl sind in den meisten Fällen kreative Daten betroffen, die unstrukturiert auf Fileservern liegen. Aktuell hat eine Studie der Wirtschaftsprüfungsgesellschaft KPMG belegt, dass Innentäter in Unternehmen leichtes Spiel haben. Besonders mittelständische Unternehmen weisen bei der Vergabe von Rechtevergaben Defizite auf. Aus diesem Grund steht Risikoprävention bei Datenzugriffen ganz oben auf der Liste deutscher Betriebe. Von den 300 befragten Unternehmen gaben 87 Prozent an, ihr Berechtigungsmanagement überarbeiten zu wollen. Zur Verwaltung von Rechtevergaben teilen Administratoren und Helpdesk-Leiter Zugriffs- und Bearbeitungsmöglichkeiten auf Dateien, Ordner und Gruppen, auf Fileservern oder NAS-Devices ein. Nur Befugnisse zu vergeben, sichert Daten aber nicht ausreichend vor unbefugtem Zugriff. Genau dies passiert jedoch häufig, weshalb die Rechteverwaltung in Unternehmen gravierende Schwachstellen aufweist. Schätzungen zufolge haben

über 90 Prozent der Mitarbeiter zu viele Zugriffsrechte.

### Verwaltungschaos im Active Directory

Windows Bordmittel reichen häufig nicht aus, um effizient und ganzheitlich strukturiert zu arbeiten. Die oft eingesetzte Minimallösung in Form von Excel-Tabellen erlaubt zwar einen Überblick, verursacht aber bei Änderungen so viel Aufwand, dass die Protokollierung meist nicht lange konsequent mitgeführt wird. Einzelne Informationen zu finden oder übersichtliche Strukturen einzuhalten, ist zu kompliziert. Das kann auch bei der Einhaltung gesetzlicher Anforderungen von Bedeutung sein. In Unternehmen ohne strukturiertes System für das Berechtigungsmanagement kann in Schadensfällen unter Umständen nicht eindeutig nachvollzogen werden, wer verantwortlich ist. Um im Fall einer Wirtschaftsprüfung umgehend einen vollständigen Report zu liefern, müssen Com-

pliance-Vorgaben jederzeit erfüllt werden. Im Mai 2010 nannte eine Studie von CA Technologies jedoch als gravierende Compliance-Hindernisse zu viele manuell durchgeführte Vorgänge und Zeitmangel bei der Bearbeitung von Prozessen. Im Idealfall funktioniert eine Recheorganisation nach dem „Need-to-know-Prinzip“ bei dem Mitarbeiter so viele Informationen bekommen, wie sie für ihre tägliche Arbeit brauchen, aber sowenig, dass ein Sicherheitsrisiko weitestgehend ausgeschlossen werden kann. Die tägliche Administration von Berechtigungen sollte sich mit geringem Zeitaufwand umsetzen lassen. Dazu sind Software Applikationen sinnvoll, die Mehrfachaufwendungen vermeiden. Dies belegte bereits 2007 eine gemeinsame Studie des Lehrstuhls für Betriebswirtschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg und Novell. Der Lehrstuhl für Betriebswirtschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg hat gemeinsam mit Novell in einer aktuellen Studie (Vorteile und Her-

ausforderungen IT-gestützter Compliance-Erfüllung) die Anforderungen, Herausforderungen, Ansätze und Strategien sowie Kostentreiber der Umsetzung von Compliance-Richtlinien untersucht und deren Nutzen identifiziert.

Softwaregestützte Compliance-Lösungen finden am Markt immer mehr Interessenten. Grund dafür sind zunehmende Ansprüche an Sicherheit. Unternehmen stehen verstärkt im Zwang, sich mit dem Thema Compliance auseinanderzusetzen, um externe und interne Bedrohungen sowie gesetzliche Anforderungen zu erfüllen. IT-Lösungen bieten mit automatisierten Vorgängen eine Unterstützung bei Sicherheit und Compliance. Wie bei jedem IT-Projekt stellt sich den Unternehmen dabei die Frage nach dem Verhältnis von Kosten und Nutzen.

## Identity-Management als Lösung

Unternehmen ab 5.000 PC-Nutzern setzen vielfach Identity Management Lösungen ein. Sie bieten vielfältige Organisationsmöglichkeiten, die von einem einfachen Verzeichnisdienst bis zu komplexen Workflow-Prozessen reichen. Zum Aufgabenbereich der Lösung kann auch die Organisation von Berechtigungen gehören. Solche Lösungen gehen nach dem Top-down-Ansatz vor. Nach Analyse der Ist-Zustände von Prozessen und Ressourcen werden Zugriffsrechte festgelegt. Auf diese Weise lassen sich die Berechtigungen auch in einem größeren Kontext betrachten und an andere Applikationen anpassen. Allerdings kann die unternehmensweite Einführung einer Identity-Management-Lösung lange dauern. Viele mittelständische und große Unternehmen scheuen den Einsatz aus Angst vor Kosten und zeitlichem Aufwand, dadurch verzichten sie auch auf ein Berechtigungsmanagement. Wer auf die Eingliederung in ein großes Management-Framework

verzichten kann, bekommt Berechtigungsmanagement auch als Stand-Alone Anwendung. Solche Programme arbeiten mit dem Bottom-up Ansatz. Dabei analysiert die Software bei der Installation selbstständig den Ist-Zustand der gesamten Berechtigungslage. Einsetzbar ab 100 Nutzern im Active Directory schließt Berechtigungsmanagement-Software die Lücke zwischen komplexen IdM-Lösungen und manueller Rechtevergabe.

Wichtig ist, dass so eine Software die Übersicht durch klare visuelle Strukturen erleichtert und Administratoren und IT-Leitern die Chance gibt, die Gesamtlage aller Berechtigungen und Einzelberechtigungen zu erfassen. Wenn die Benutzeroberfläche leicht zu bedienen ist, können Leiter von Fachabteilungen, Eigentümer der Daten sowie Helpdesk-Leiter selbst Berechtigungen einsehen und vergeben. Dadurch beeinflussen genau die Personen die Rechte, die die Zuständigkeit der entsprechenden Mitarbeiter am besten kennen.

## Warnungen bei Konflikten

Eine bestimmte Berechtigung oder alle geltenden Freigaben für einen Mitarbeiter zu finden, ist mit einer visualisierten Darstellung einfacher. Weil viele Aufgaben für Mitarbeiter und Gruppen identisch sind, können solche Programme auch oft automatisiert werden. So eine Standardisierung der Systemabläufe erleichtert auch präventive Handlungen im Risikomanagement. Rechekonflikte durch Vererbung oder widersprüchliche Gruppenmitgliedschaften führen zu Warnungen und werden im Ansatz verhindert.

Abteilungs- oder Positionswechsel, Stellvertretungen und der Verlauf von Ausbildungen führen zu geänderten Situationen der Berechtigungslage. Neue Rechte kommen hinzu und alte müssen unter Umständen aufgehoben werden.



Stephan Brack, Geschäftsführer protected-networks.com GmbH

Auch das „Auszubildenden-Problem“ lässt sich durch eine Software zum Berechtigungsmanagement lösen. Dazu wird bereits am Anfang einer Rechtevergabe ein Zeitraum festgelegt, nach dessen Ablauf die Ursprungssituation wieder hergestellt wird.

Durch die Möglichkeit, die Personalabteilung selbst Rechte erteilen und auch wieder entziehen zu lassen, sinkt die Wahrscheinlichkeit, dass „Karteileichen“ nach dem Ausscheiden aus der Firma weiterhin über Rechte verfügen, die von Angreifern ausgenutzt werden könnten.

Hilfreich für alle Vorgänge im Berechtigungsmanagement ist die automatische Dokumentation von Softwarelösungen. Protokolle zeichnen jede Aktion auf, sodass rückblickend nachvollzogen werden kann, welche Person zu einem bestimmten Zeitpunkt ein kritisches Zugriffsrecht innehatte oder vergeben hat. Alle relevanten Daten zu Person, Zeit, Datum und Aktion sind gespeichert und lassen sich auf Wunsch nachvollziehen. Aussagekräftige Berichte für Wirtschaftsprüfungen oder Geschäftsleitung verursachen mit Hilfe dieser Reports nur sehr wenig Aufwand. Wer Compliance ernst nimmt, sollte das Berechtigungsmanagement ebenfalls ernst nehmen. ■