«Eine gute Rollenmodellierung – Was heisst das?»

In der heutigen IT gewinnen Fragen zu mehr Sicherheit, Überwachung und Automatisierung von Systemzugriffen immer mehr an Relevanz. Zugriffe über eine rollenbasierte Zugriffssteuerung (RBAC) gelten immer mehr als Selbstverständlichkeit und sind für viele Firmen nicht mehr wegzudenken, da dieses Vorgehen in guter Ausführung die genannten Probleme zu einem weiten Grad löst. Dieser Artikel liefert und verdeutlicht den Ansatz von guter Rollenmodellierung und beschreibt welche Punkte hierfür wichtig sind. Eine Zugriffssteuerung basierend auf Rollen rechnet sich aus Gründen wie Effizienzsteigerung, Automatisierung, Verbesserung der Compliance und generell tieferen Administrationsaufwänden und ist eine lohnende Investition für die Zukunft.

Keywords - Rollenmodellierung, Rolemodeling, RBAC, ABAC, Rollendesign, SoD, IAM, Cloud Computing, IT Governance

Einleitung

34% aller IT Schwachstellen stehen in Zusammenhang mit Zugriffskontrollen oder der darin enthaltenen fehlenden Trennung von Funktionen (SoD) (Hermanson 2007). Diese Schwachstellen basieren auch direkt oder indirekt auf der Art der Rollenmodellierung. Viele Firmen sehnen sich nach einer einfachen, übersichtlichen und automatisierten Zugriffsregelung für ihre IT Systeme. Oftmals wird hierbei auch von „Identity Governance“ oder generell einer klaren IT Governance gesprochen, die Policy-basierte Regulierungen für das Identitätsmanagement und Zugangskontrolle schafft und vorgibt. Häufig führen Prozesse wie Mitarbeitereintritte, Mitarbeiteraustritte und Reorganisationen zu einer unübersichtlichen Rechteverwaltung auf den Systemen und bilden somit auch Gefahr für Betrug.

Zudem werden durch den Einfluss von Cloud Computing Systemlandschaften und Zugriffsmuster in den Firmen verändert. Auch hierfür werden gute Rollenmodellierungen und möglichst sichere Zugriffsmodelle immer notwendiger. Durch Veränderungen von Systemlandschaften braucht es veränderte Denkmuster und neue Anforderungen an das Rollendesign und Zugriffsregelungssysteme. Der Stellenwert einer guten Rollenmodellierung erhöht sich (Nichols 2011).

Eine manuelle Rechtevergabe bedeutet oft ständig wiederkehrende Administrationsaufwände für das IT Team. Um den Prozess effizienter zu gestalten ist eine Zugriffsverwaltung basierend auf Rollen und automatisierter Zugriffsvergabe der richtige Weg. Zugriffe über eine rollenbasierte Zugriffssteuerung (RBAC) zu verwalten ist für viele Unternehmen nicht mehr wegzudenken, da die Berechtigungsvergabe nach logischer Rechtezusammengehörigkeit hierarchisch und nutzungsorientiert ermöglicht wird. Ausserdem werden Sicherheitsrisiken vermindert.

Abbildung 1 zeigt die Gegenüberstellung von direkter Rechtevergabe und der Rechtevergabe über Benutzerrollen mit den Beispielrollen „Buchhalter“ und „Lagerarbeiter“.

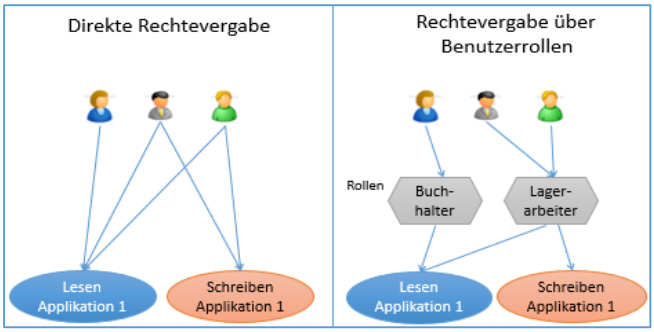

Abbildung 1: Rechtevergabe über Benutzerrollen

Problemstellung und Ziele

Berechtigungen auf den Systemen sind vergeben, aber es mangelt an Übersichtlichkeit. Das Beantragen von Berechtigungen für Zielsysteme ist zeitintensiv und die Automatisierung der Prozessvorgänge ist nicht oder nur erschwert möglich. Eine Einhaltung der Compliance, inklusive der klaren Trennung von Funktionen (Segregation of Duties - SoD) ist zudem nicht oder nur schwer möglich.

Ziel ist es eine Zugriffssteuerung über RBAC zu erreichen, die eine Einhaltung der Compliance ermöglicht und Standards für sichere Zugriffe schafft. Weitere Ziele sind das automatisierte Verwalten der Berechtigungen und effiziente Prozesse.

Faktoren für eine gute Rollenmodellierung

Erfahrungsgemäss beinhaltet eine gute Rollenmodellierung folgende zentrale Punkte:

- **Klare Business und Compliance Ziele:** Definition von klaren Zielen und Abgrenzungen, die mit der Rollenmodellierung erreicht werden sollen.
  - ✓ **Erreichung Compliance**
  - ✓ **Funktionstrennung (SoD)**
  - ✓ **Risiko Reduzierung**
  - ✓ **Automatisierung der Prozesse**
  - ✓ **Automatische Zuweisung der Rollen**
  - ✓ **Anforderungen und Projektumfang**
  - ✓ **Effizienz erhöhen und Kosten reduzieren**

- **Einbezug wichtiger Stakeholder**: Einbezug der Verantwortlichen aus Business und Compliance, um die Art und die Behandlung von Rollen zu klären.
- **Definition Rollentypen**: Definition der Rollentypen, die modelliert werden sollen. Klarer Ausschluss der Rollentypen, die nicht benötigt werden (Trade-Off).
- **Automatische Zuweisung der Rollen**: Festlegung eines ausgewogenen Verhältnisses, welche Rollen automatisch vergeben und welche Rollen manuell vom Endbenutzer beantragt werden müssen.
- **Verbundenes Vorgehen Top-Down und Bottom-Up**: Analyse der existierenden Zugriffsrechte (Bottom-Up) mit gleichzeitigem Festlegen von Rollen nach Funktionsprofil und Position (Top-Down) sind Vorgehen, die verbunden werden müssen. Das verbundene Vorgehen wird auch Middle-Out oder Hybrid-Ansatz genannt.
- **Verständliches Rollenmodell**: Aufbau einer verständlichen Struktur und Hierarchie. Es ist gerade zu Beginn der Rollenmodellierung von grosser Bedeutung, die Rollen in Business-, Applikation-, und Systemrollen zu klassifizieren und eine sinnvolle und logische Bündelung von Rollen aufzubauen. Dies bewirkt sowohl eine klare als auch logische Trennung von organisatorischer, applikatorischer und technischer Sicht, als auch die strukturierte Beziehungen untereinander.
- **Rollenvalidierung**: Das Erstellen von Rollen benötigt immer auch eine Prüfung und Freigabe der Rollen durch festgelegte Verantwortliche. Eine Definition der zu prüfenden Validierungsformen muss erarbeitet werden.
- **„Role Life Cycle"**: Die Rollenerstellung ist nur der Start eines Lebenszyklus einer Rolle („Role Life Cycle"). Es sind nachfolgend weitere Schritte bei der Modellierung zu beachten. Zudem müssen Rollen auch kontinuierlich überprüft und überarbeitet werden, um neuesten Anforderungen zu genügen.
- **Leitfaden „Rollenmodellierung"**: Wichtig für den Erfolg der Rollenmodellierung ist es, für das Vorgehen einen klaren Leitfaden zu etablieren und zu beachten.
- **Einbindung von externem Praxis Knowhow**: Ein Garant für eine erfolgreiche Rollenmodellierung ist auch die Einbindung externer Spezialisten, die mit ihren Erfahrungen und ihren best-practice Ansätzen hilfreiche Unterstützung leisten können.

Schlussfolgerungen

Anforderungen an Sicherheit, Compliance und an Automatisierung der Systemzugriffe werden in der heutigen IT-Welt immer bedeutender. Mit einer guten Rollenmodellierung kann eine durchgängige rollenbasierte Zugriffssteuerung (RBAC) erreicht werden. Sie ist eine wichtige Schlüsseldisziplin und bildet die Basis für eine spätere Implementierung einer IAM-Lösung. Das Bewusstsein und Wissen was eine gute Rollenmodellierung ausmacht und wie man vorgeht ist für den Erfolg von entscheidender Bedeutung. Diverse Faktoren und Schlüsselaufgaben hierfür wurden in diesem Fachartikel präsentiert. Mit Einhaltung der methodischen Umsetzung und Beachtung der wichtigsten Faktoren, ist die Rollenmodellierung ein wertvolles Instrument für die sichere und effiziente Rechtevergabe auf Basis von Rollen. Folgende Ziele werden damit erreicht:

1) Transparenz über die aktuellen Berechtigungs-vergaben,
2) Vorrausetzung für automatisiertes Vergeben oder Entziehen von Rollen, zum Beispiel bei Mitarbeiter-eintritt oder –austritt,
3) Einhaltung der IT-Governance & Compliance,
4) Einsparen von Administrationsaufwänden
5) das Potential für eine merkliche Effizienzsteigerung der Geschäftsprozesse.

Über den Autor

Daniel Kappeler
WiB Solutions AG

Daniel Kappeler ist ICT Consultant bei WiB Solutions AG in den Bereichen Rollenmodellierung, Business-Analyse, Anforderungserhebung und IAM-Beratung. Eine analytische Vorgehensweise sowie die Betrachtung von unterschiedlichen Business und IT Standpunkten sind bedeutende Faktoren für ihn.

Quellenangaben

1. Hermanson, D., Ivancevich, D., Ivancevich, S., 2007. *IT-Related Material Weaknesses In Internal Control: Initial Evidence From SOX Section 404 Reports*
2. Nichols, K., Sprague, K., 2011, *Getting ahead in the cloud*
3. Osmanoglu, E, 2014. *Identity and Access Management. Business Performance Through Connected Intelligence*
4. Verschiedene Unterlagen aus Projekterfahrungen der WiB Solutions AG