«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“.

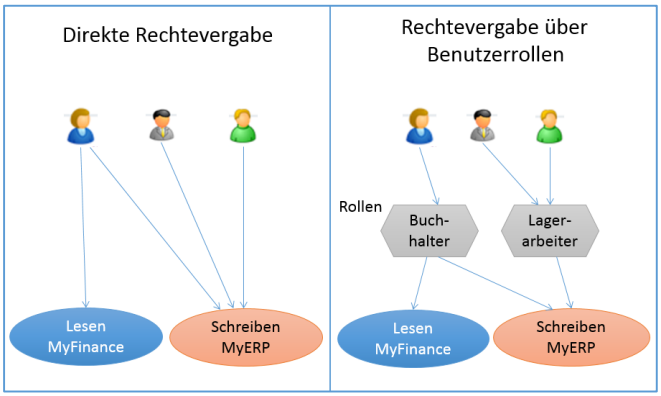

Abbildung 1: Rechtevergabe über Benutzerrollen

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 Ziele:** Definition von klaren Zielen und Abgrenzungen, die mit der Rollenmodellierung erreicht werden sollen.
- **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 auto-

matisch 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.

Das Beachten und das Einbinden all dieser Faktoren sind sehr wichtig. All diese Faktoren werden im Detail und zum Teil anhand eines Beispiels im nächsten Abschnitt spezifischer erläutert.

Praxis-Exkurs: Rollenmodellierung unter Berücksichtigung der Faktoren

Mitarbeiter eines Logistikunternehmens (z.B. „MyLogistics") benötigten Zugriffe auf verschiedene Systeme, zum Beispiel ein ERP-System (z.B. „MyERP") und ein Finanz-System (z.B. „MyFinance"). Es werden diverse Rollen für den Zugriff auf diese Systemen benötigt, im Beispiel eine Funktionsrolle „Buchhalter" und eine Funktionsrolle „Lagerarbeiter". In *Abbildung 1* wurden diese Systeme und Rollen schon kurz erwähnt.

Klare Business und Compliance Ziele

Die Anzahl und der Umfang der Business Anforderungen haben einen entscheidenden Einfluss auf die Grösse des Rollenmodellierung-Projekts. Folgende Business Ziele sind aus Erfahrung für viele Kunden zentral:

- **Erreichung Compliance**: Definition der Ziele für die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft. Diese müssen in einem ausgewogen Kosten-Nutzen-Verhältnis festgelegt werden.
- **Funktionstrennung (SoD)**: Ein besonderes Augenmerk muss auf das strikte Trennen von sich ausschliessenden Rollen gerichtet werden. Im Beispiel darf der Lagerarbeiter nicht gleichzeitig die Rolle des Buchhalters zugewiesen bekommen. Dies bedeutet es muss klar definiert werden, welche Rollen sich gegenseitig ausschliessen, welche für Benutzer überhaupt auswählbar sind und welche Genehmigungsprozesse für sensible Rollen, wie z.B. die des Buchhalters, notwendig sind. (z.B. Vier-Augen-Prinzip). Oft ist SoD ungenügend definiert, was zu Betrugsmöglichkeiten führt dadurch dass solche Szenarien möglich sind.
- **Risiko Reduzierung**: Missbrauch und die Wahrscheinlichkeit von Fehlern festzustellen, ob absichtlich oder unabsichtlich, ist für diverse Firmen von grosser Bedeutung. Eine hohe Risikominimierung und Prävention wird durch eine standardisierte Rollenmodellierung erreicht, jedoch definiert der Kunde aufgrund seiner Anforderungen, zu welchem Grad eine Risikominimierung stattfinden sollte.
- **Automatisierung der Prozesse**: Schon im Vorfeld sollte der gewünschte Grad der Automatisierung festgelegt werden und evaluiert werden, welche Lösung die Anforderungen am besten abdecken kann. Die Rollenmodellierung liefert die Grundlage für eine Automatisierung mit einem IAM-System.
- **Automatische Zuweisung der Rollen**: Es ist möglich Rollen an Benutzer nach Benutzerkriterien automatisch zu vergeben. Ein gewisser Teil der Rollen wird dem Endbenutzer zur Beantragung zur Verfügung gestellt. Es soll jedoch eine möglichst hohe Anzahl an automatisch zugewiesenen Rollen (auch Automatisierungsgrad genannt) erreicht werden. Viele Firmen streben bei der Automatisierung einen Wert von 80% an. Höhere Werte des Automatisierungsgrades bedeuten zwar eine langfristige bessere Prozesseffizienz, führen jedoch auch zu höherem Aufwand in der Rollenerstellung. Hier ist es relevant die Anforderungen und Ziele aus dem Business genau zu kennen und Kosten und Nutzen in Relation abschätzen zu können.
- **Anforderungen und Projektumfang**: Die Art der Anforderungen hat einen grossen Einfluss auf den Projektumfang. Die meisten Projekte scheitern schon beim Projektantrag, da zu viele Ziele mit einem Schritt erreicht werden sollen. Je nach Budget muss eventuell auf kostenintensive Umsetzungen von Anforderungen verzichtet werden. Beispielsweise könnte im ersten Schritt auf die automatisierte Rollenzuweisung oder die Überwachung von Konsistenzerhaltung auf Systemen (Reconciliation) verzichtet werden.
- **Effizienz erhöhen und Kosten reduzieren**: Eine gute Rollenmodellierung erhöht die Effizienz in der Rechtevergabe, senkt unmittelbar die Kosten durch einen geringeren administrativen Aufwand und vereinfacht die Durchführung von Audits.

Einbezug wichtiger Stakeholder

Für den Projekterfolg ist es absolut notwendig die wichtigsten Stakeholder in das Projekt einzubeziehen. Mitarbeiter aus dem Business werden benötigt, um konkrete Anforderungen zu erheben. Compliance Verantwortliche müssen den erforderlichen Grad an Sicherheit, Regulierungs- und Auditanforderungen definieren. Zudem werden zusätzlich interne IT-Fachkräfte benötigt, z.B. für Tool-unterstützung oder für die Datenlieferung der existierenden Berechtigungen.

Definition Rollentypen

Es gibt viele verschiedene Rollentypen, die verwaltet werden könnten. Der Rollentyp definiert unterschiedliche Formen einer Rolle. Beispiele für Rollentypen sind „Generelle Rollen“, „Funktionsprofile“, „Organisationen“, „Standorte“, „Positionen“, „Applikationsfunktionale Rollen“, „Projekt-funktionale Rollen“ oder „Service Rollen“.

Für die Firma „MyLogistics“ könnten z.B. „Generelle Rollen“, „Positionen“ und „Funktionsprofil“ Sinn machen. *Abbildung 2* beschreibt Beispiele für die genannten Rollentypen.

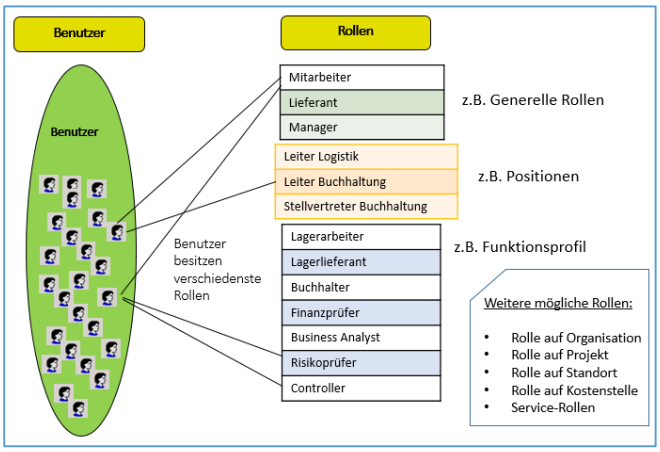

Abbildung 2: Zuweisung von Rollen

Die Definition von Rollentypen ist oft sehr kundenspezifisch. Je nach Branche und Organisationsaufbau braucht es unterschiedliche Rollentypen. Das Festlegen der Rollentypen, auf die man fokussieren will, ist eine elementare strategische Entscheidung, die sehr früh im Rollenmodellierungsprozess getroffen werden muss.

Automatische Zuweisung der Rollen:

Automatisierung bedeutet, dass abhängig von gewissen Attributen (z.B. Organisationen oder Funktionen), Rollen automatisch an Benutzer vergeben werden können. Dies geschieht automatisch - ohne Rollenbeantragungsprozess. Es bieten sich verschiedene Attribute zur Automatisierung der Rollenzuweisung an. Je nach Anforderung macht es Sinn, den Automatisierungsgrad zu Beginn eher tief zu halten und dann kontinuierlich auszubauen. Ein höherer Auto-matisierungsgrad bedeutet zwar eine langfristig bessere Prozesseffizienz, führt jedoch auch zu höheren Projekt-aufwänden. Es ist zu empfehlen den Automatisierungsgrad als Startziel eher auf 60% zu definieren und diesen in Richtung 80% weiterzuentwickeln. Die Entwicklung ist meist durch die Anforderungen im Projekt vorgegeben. Je nach Treiber ist es notwendig, möglichst schnell einen hohen Automatisierungsgrad zu erreichen. Es gilt: eine gute Rollenmodellierung ist ein kontinuierlicher Entwicklungs-prozess und keine Endlösung.

Verbundenes Vorgehen Top-Down und Bottom-Up:

Bei der Top-Down Vorgehensweise werden Rollen (ohne bestendende Daten) basierend auf dem Nutzen in einer Organisation festgelegt – eine eher betriebswirtschaftliche Perspektive. Bei der Bottom-Up Vorgehensweise, werden die bestehenden Zugriffsrechte geprüft (z.B. aus Active Directory) und basierend auf diesen Daten Rollen erstellt – eine eher technische Perspektive. Beide Vorgehen mitein-ander verbunden machen eine gute Rollenmodellierung aus. Hierbei können die beiden Vorgehensweisen unterschiedlich gewichtet werden. Je nachdem wie hoch der Zufrieden-heitsgrad mit den bestehenden Berechtigungsständen ist, gilt üblicherweise entweder Top-Down oder Bottom-Up als treibende Kraft.

Verständliches Rollenmodell:

Ein Rollenmodell schafft eine bessere Übersichtlichkeit und reduziert die Komplexität. Viele einzelne Rechte können in Businessrollen zusammengefasst werden und hierarchisch aufgebaut sein. Der administrative Verwaltungsaufwand wird drastisch reduziert, wenn Rollen anstatt Einzelrechte „bestellt“ werden können. Dies erfordert jedoch aussage-kräftige und verständliche Namen, sowie ein logisches und allen bekanntes Rollenmodell. Weitere Benefits sind eine kürzere Einrichtungszeit und eine Entlastung des Help Desk.

Systemrollen sind Rollentypen, die Berechtigungen auf Systemen beinhalten. Sie enthalten Einzelrecht, wie z.B. „Schreiben“ oder „Lesen“ auf einem System oder Fileshare. Applikationsrollen sind Rollentypen, die eine Bündelung von Systemrollen zu einer Applikation, z.B. MyFinance oder MyERP enthalten. Eine Businessrolle ist die einzige Rolle, die für Benutzer beantragbar sein darf. Eine Businessrolle bündelt normalerweise Applikationsrollen, kann aber auch Businessrollen enthalten. *Abbildung 3* zeigt diese Rollenhierarchie (oder auch Rollenbaum genannt) anhand der Beispielapplikationen für die Rolle Businessrolle „Buchhaltung“.

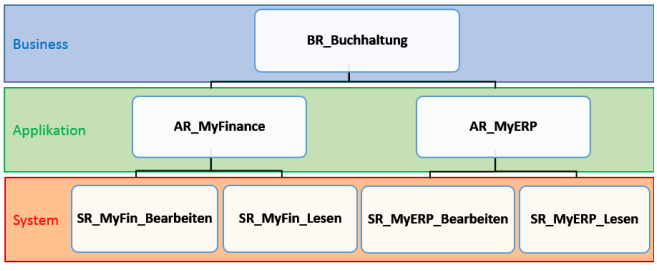

Abbildung 3: Rollenbaum

Abbildung 4 zeigt ein Beispiel mit möglichen Zuweisungen von Businessrollen an Benutzer. Eine Bündelung von verschiedenen Rollen kann zu nützlichen übergeordneten Rollen führen. Mit der Rolle „Teamleitung SchreibenLesen“ wird beispielsweise ein Schreiben und Lesen auf alle benötigten IT Systeme von Buchhaltung, Controlling, Lager und Spedition ermöglicht.

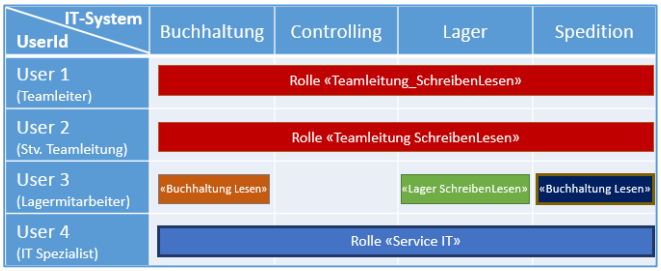

Abbildung 4: Zuweisung von Businessrollen

Eine Lösung, die eine moderne rollenbasierte Zugriffssteuerung über RBAC (Role-Based Access Management) erlaubt, unterstützt meist auch eine Zugriffsteuerung über ABAC (Attribute-Based Access Management). Mittels ABAC wird der Zugriff auf IT-Systeme über Attribute, wie z.B. den Standort eines Benutzers ermöglicht. Zugriffe über ABAC haben in Banken und Versicherung oft sehr dynamische Daten und Applikationssicherheiten als Basis. Beispielsweise würde es keinen Sinn machen für jeden Standort mit einem Kassierer oder Kundenberater eine eigene Rolle zu erstellen. Je nach Standort darf jeder Kassierer oder Kundenberater nur Zugriff auf die lokalen Sichten der IT-Systeme mit seinen Standortbefugnissen erhalten. Mit RBAC müssten hunderte von Rollen erstellt werden. Für solch komplexere Szenarien mit attributabhängigen Zugriffen kommt ABAC zum Einsatz.

Rollenvalidierung

Bei der Rollenvalidierung müssen verschiedene Validierungsobjekte festgelegt werden, die zwingend beachtet und weiterverfolgt werden müssen. Dies können z.B. „Kombinationen von Rollen“, „Sensitive Daten“, „SoD Fälle“ oder „Approval Prozesstypen“ sein. Es muss festgelegt werden, welche Mitarbeiter aus dem Compliance Team für diese Prüfungen verantwortlich sind.

„Role Life Cycle“

Rollenmodellierung ist ein kontinuierlicher Prozess. Zuerst werden die Rollen entwickelt (Role Engineering), danach folgt eine Übergabe an den Rollen-Owner. Anschliessend wird die Art des Zugriffsantrags festgelegt. Ein Beispiel hierfür wäre die Entscheidung, ob eine beantragte Businessrolle automatisch oder manuell eingerichtet wird. Nach Abschluss dieses Prozessschritts werden die Sensitivität einer Rolle, die Anzahl der Genehmigungsschritte und die Verantwortlichen seitens Compliance und Risk Management festgelegt. Der letzte Schritt im „Role Life Cycle“ enthält die periodische Prüfung der Rollen und führt wieder zum ersten Schritt des Role Engineering Prozesses (Reengineering). In der Praxis sollte ein regelmässig durchgeführter Attestation-Prozess zur periodischen Überprüfung aller Rollen etabliert werden.

Abbildung 5 zeigt diesen „Role Life Cycle“ mit seinen fünf beschriebenen Schritten.

Abbildung 5: "Role Life Cycle"

Leitfaden „Rollenmodellierung“

Wichtig ist bei der Rollenmodellierung stets einen Überblick über das Vorgehen bei der Rollenmodellierung zu behalten. Ein Rollenmodellierungsprojekt braucht Struktur und einen guten Leitfaden. Aus Erfahrung ist es zu bevorzugen ein Projekt in mehrere Phasen aufzuteilen und methodisch nach Leitfaden vorzugehen.

Abbildung 6 zeigt einen Leitfaden und die einzelnen Projektschritte. Die stärksten Schlüsselfaktoren für eine gute Rollenmodellierung sind fett markiert.

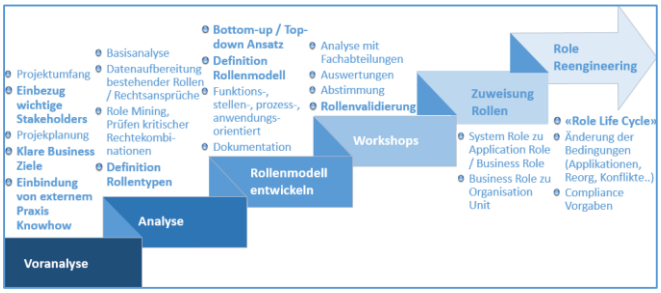

Abbildung 6: Leitfaden „Rollenmodellierung“

Weil ein Rollenmodellierungsprojekt verschiedene Projektschritte enthält, ist die Unterstützung anhand eines Leitfadens sehr nützlich. Dieser hält Meilensteine fest und bietet eine gute Übersicht über die zu tätigen Aufgaben. Die Erstellung eines kundenspezifischen Leitfadens ist zu empfehlen. Insbesondere dient der Leitfaden zur Kontrolle der Schlüsselaufgaben.

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 Berechtigungsvergaben, 2) Vorrausetzung für automatisiertes Vergeben oder Entziehen von Rollen, zum Beispiel bei Mitarbeitereintritt oder –austritt, 3) Einhaltung der IT-Governance & Compliance, 4) Einsparen von Administrationsaufwänden und 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 wichtige 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