Optimale Zugriffkontrolle sowie Trennung von Funktionen und Aufgaben

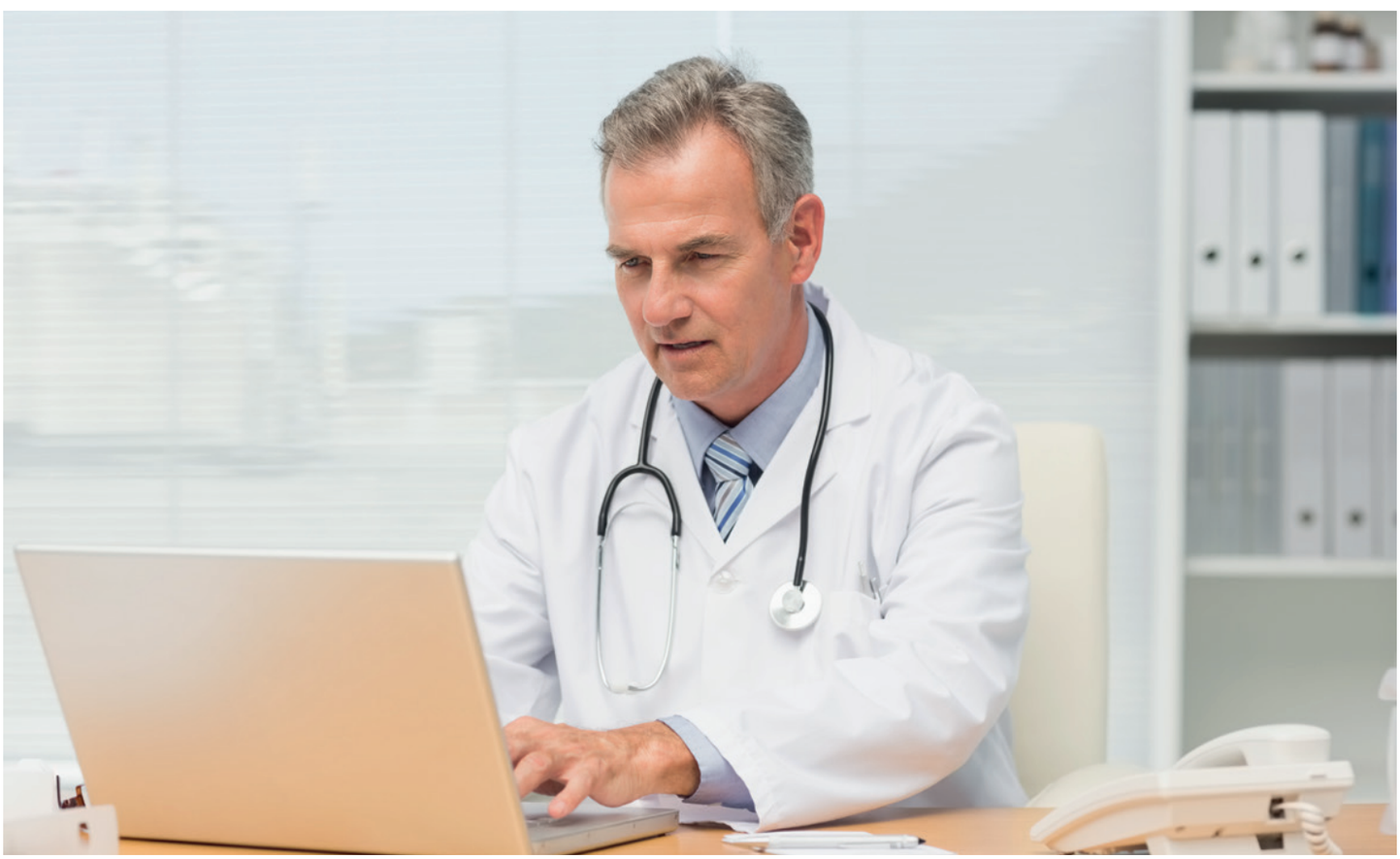
Rollenmodelle verbessern die IT-Sicherheit

Ein signifikanter Teil aller IT-Schwachstellen ergibt sich durch eine ungenügende Zugriffskontrolle oder die fehlerhafte Trennung von Funktionen und Aufgaben der Mitarbeiter (Segregation of Duties – SOD). Ohne Behebung dieser Schwachstellen laufen Unternehmungen in Gefahr, dass vertrauliche Daten, wie bspw. Patientendossiers, in die Hände von unautorisierten Personen gelangen. Ein Umstand, der nicht zuletzt seit der Implementierung der DSGVO (Datenschutz-Grundverordnung) mit hohen Bussen (bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes) sanktioniert werden kann.

Besonders Prozesse wie der Ein- oder Austritt von Mitarbeitenden oder Reorganisationen führen zu Unübersichtlichkeiten, die das Risiko für unbefugte Zugriffe erhöhen. Zudem verändern Cloud-Computing Systemlandschaften die Zugriffsmuster in Firmen, da die Mitarbeitenden von überall über alle möglichen Geräte auf potenziell sensible Daten zugreifen können. Eine Lösung für diese Probleme bietet die rollenbasierte Zugriffssteuerung (Role Based Access Control – RBAC).

Zugriffe rollenbasiert und automatisch gewähren

Diese verfolgt den Ansatz, wie der Name bereits andeutet, Zugriffe rollenbasiert und weitestgehend automatisiert zu gewähren um damit menschliche Fehler auszuschliessen. Die Zugriffsberechtigungsvergabe wird anhand von logischen Berechtigungsrelationen hierarchisch und nutzungsorientiert nach den Vorgaben der IT-Governance implementiert. Dadurch erhöhen sich die Transparenz und Nachvollziehbarkeit der Zugriffe; wobei, als Nebeneffekt, durch automatisierte Prozesse der Administrationsaufwand für die IT-Mitarbeitenden minimiert wird.



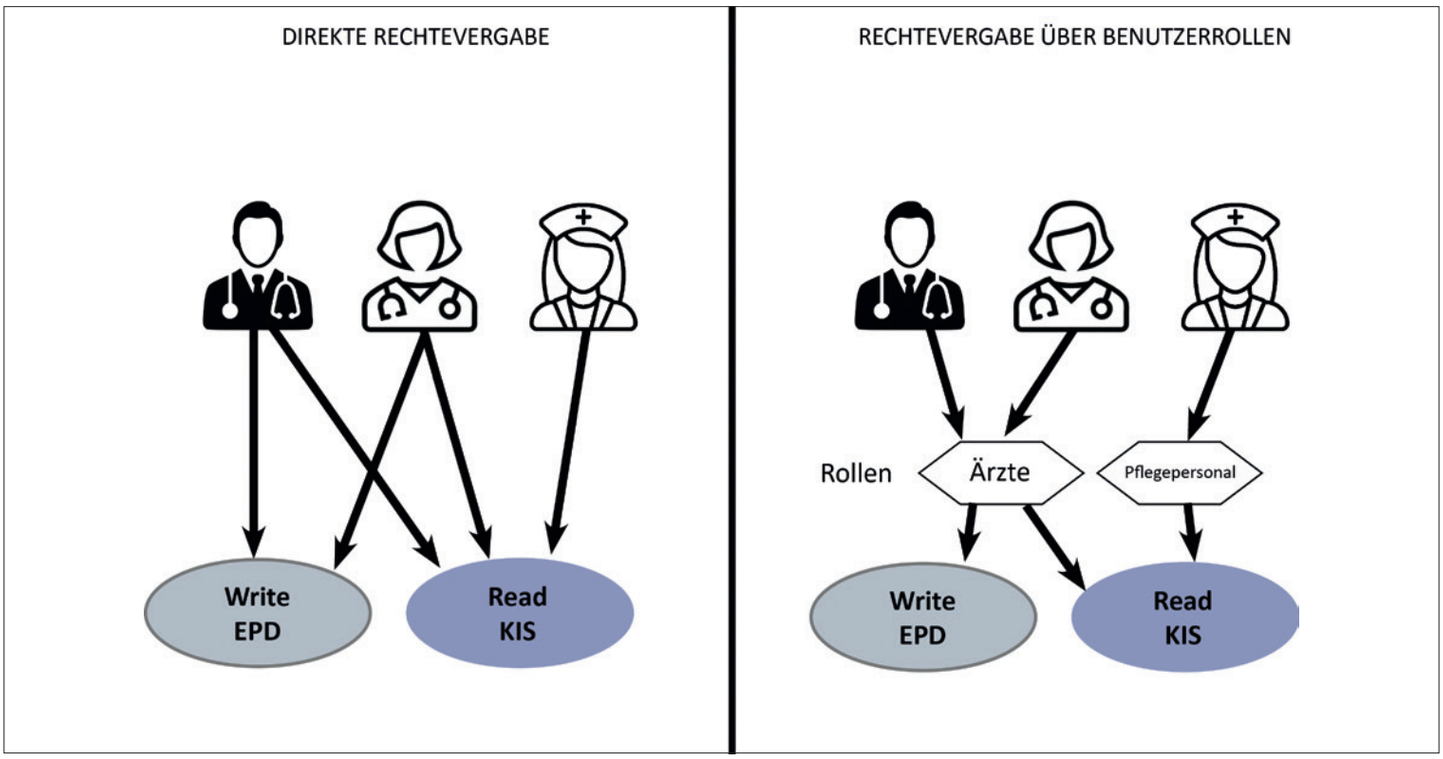


Abbildung 1: Zugriffsschemata mit und ohne RBAC

Zwei Schemata auf dieser Seite zeigen die manuelle Berechtigungsvergabe (links) und mittels RBAC (rechts). Die manuelle Vergabe ist flexibel, dafür fehleranfälliger und zeitintensiver. Für jede Benutzeridentität sind alle Einzelberechtigungen einzeln zu identifizieren und zuzuweisen. Mit RBAC haben die User die Möglichkeit, Einzelberechtigungen in Rollen zu bündeln. Die konzipierten Rollen können über Policies (Richtlinien zur Vergabe) an die zu begünstigenden Benutzeridentitäten provisioniert, bzw. zugewiesen werden. Dies, da Mitarbeitende beim Eintritt in eine Unternehmung mit Attributen versehen werden, wie der Organisationseinheitszugehörigkeit oder der Funktion. Je nach Ausprägung dieser Attribute werden dem Benutzer über die definierte Policy Rollen zugewiesen. Bspw. erhalten alle Ärzte aus der Abteilung Onkologie dasselbe Set an Einzelberechtigungen; vollautomatisiert, ohne manuelle Eingriffe. Dabei gilt ein Automatisierungsgrad von 80% als erstrebenswert. Ein zu tiefer Grad vermindert den Nutzen von RBAC. Eine vollständige Automatisierung nimmt den Benutzern jegliche Flexibilität.

Erfolgsfaktoren fürs gute Umsetzen

Folgende Faktoren zu beachten um eine Rollenmodellierung richtig umzusetzen:

- **Definition von klaren Zielen aus den Gebieten Business und Compliance**: Darunter fallen Ziele wie bspw. die transparente Trennung von Funktionen (SoD), Risikoreduktion, Automatisierung von Prozessen, automatische Zuweisung von Rollen, Kosteneinsparungen, etc. unter Berücksichtigung der wirtschaftlichen und technischen Rahmenbedingungen.
- **Festlegen, welche Arten von Rollen konzipiert werden sollen**: Beispiele sind Rollen, die für spezifische Funktionen, Standorte, Organisationseinheiten, Projektfunktionen oder hierarchische Stellungen vorgesehen sind. Da die Typisierung eine elementare strategische Entscheidung darstellt, ist sie möglichst früh im Rollenmodellierungsprozess zu behandeln.
- **Definition eines gleichbleibenden Namenskonzepts**: Sprechende Namen erhöhen die Übersichtlichkeit und reduzieren die Komplexität. Eine Mitarbeitende wird eine Rolle mit Namen «EPD-Zugriff»(EPD steht für?) schneller identifizieren können, als dass sie eine Kombination aus Zahlen und Buchstaben interpretieren kann. Die oben erwähnte Typisierung, bzw. Art der Rollen kann sich auch in den Namen abbilden. So könnte man bspw. aus dem Rollennamen BR_OU_ONK ableiten, dass es sich um eine Business Role (BR) der Organisationeinheit (OU) Onkologie (ONK) handelt. Wohingegen eine BR_SPEZ_Controlling eher auf die Spezialfunktion eines Controllers aus der Finanzabteilung zielt.
- **Einbezug von Stakeholdern aus den Bereichen Business und Compliance**, um die Art von benötigten Rollen und deren Handhabung zu klären: Beispielsweise, ob die Vergabe von projektspezifischen Rollen über Policies erfolgen soll, was eine automatische Berechtigungsvergabe ermöglichen würde. Oder aber welche Art und welche Anzahl von Genehmigungsstufen für manuell vergebene Rolle definiert wird, bzw. werden.
- **Definition der zu modellierenden und (begründeter) Ausschluss nicht benötigter Rollen(typen)**: Hier geht es darum, ob beispielsweise Lernende in Ihrer Unternehmung eine spezielle Rolle erhalten sollen.
- **Festlegen, welche Rollen automatisch über Policies oder Vererbungen zugeteilt werden und welche manuell zu beantragen sind**: Nehmen wir an, ein Unternehmen habe ein neues Projekt zur Erforschung des Einflusses von Frontallappendeformationen (?) zu kriminellem Verhalten. Da nicht alle involvierten Personen vollzeitig an diesem Projekt arbeiten und das Vorhaben eine interdisziplinäre Betrachtung benötigt, machen Sie am besten eine Rolle aus allen notwendigen Berechtigungen und weisen diese den entsprechenden Mitarbeitenden bei Bedarf zu.
- **Hybrider Ansatz mit Analyse existierender Zugriffsrechte (Bottom-Up) und paralleler Modellierung von Rollen nach Funktionsprofil und hierarchischer Position (Top-**

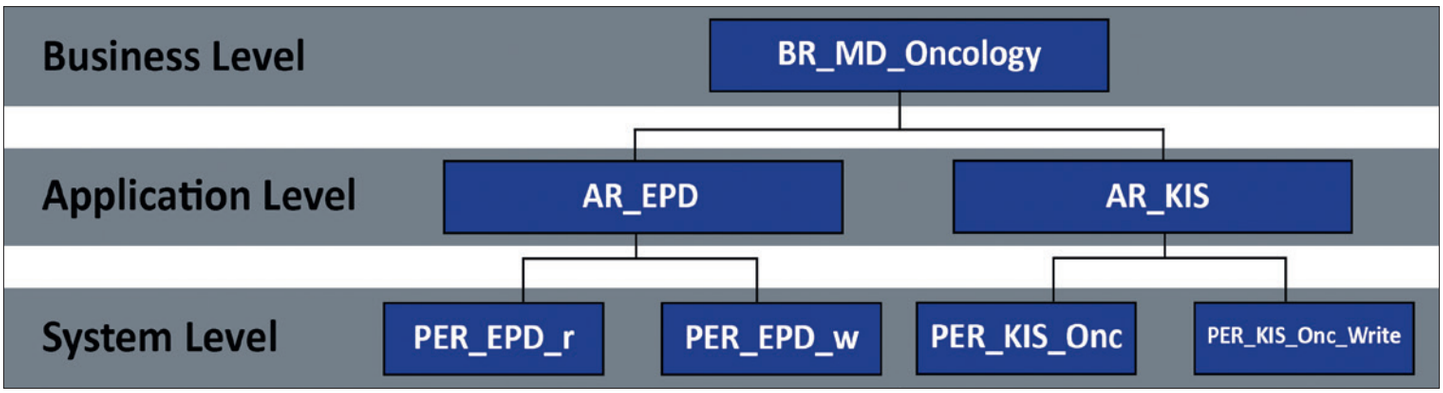


Abbildung 2: Beispiel für einen Rollenbaum

Down): Mit diesem Ansatz werden beispielsweise Informationen aus Ihrem Active Directory analysiert um mithilfe von angewandter Mengenlehre Bündelungen von Berechtigungen (sogenannte Rollenkandidaten) zu identifizieren. Somit wird eine klare Übersicht geschaffen, welche Mitarbeitenden über welche Berechtigungen in Ihrer Unternehmung verfügen. Dies bietet die Informationsgrundlage für die Konstruktion von Rollen für die zukünftige Nutzung. Die Rollenkandidaten werden anschliessend mit dem Funktionsprofil der entsprechenden Mitarbeitenden abgeglichen um schlussendlich Rollen pro Funktion zu definieren.

- **Aufbau einer nachvollziehbaren Struktur und Hierarchie**: Nebst dem, dass Einzelberechtigungen, als Bestandteile der Rollen sprechend und nachvollziehbar zu benennen sind, muss die Anbindung, bzw. die Verschachtelung von Berechtigungen in strukturierter Weise stattfinden. Nachfolgend ist ein Beispiel eines sogenannten Rollenbaums aufgeführt. Ein Arzt in der Abteilung Onkologie benötigt beispielsweise Zugriffe auf die Applikationen EPD (AR_EPD) und KIS (AR_KIS). Die Applikationsrollen werden auf höherer Ebene (auf dem Business Level) zur Business Rolle BR_MD_Oncology zusammengefasst. Der Arzt erhält nun aufgrund seiner Organisationseinheitszugehörigkeit Onkologie die Business Role BR_MD_Oncology provisioniert. Damit erhält er Zugriff auf die oben genannten Application Roles. Den Application Roles sind schlussendlich Einzelberechtigungen (System Roles auf dem System Level) angehängt (PER_KIS_Onc und PER_KIS_Onc_Write). Ein Rollenbaum kann selbstredend mehr als drei Stufen haben; frei nach Ihren Bedürfnissen. Allerdings hat die Erfahrung gezeigt, dass mind. zwei Stufen notwendig sind um genügend Flexibilität zu haben. Im Gegensatz dazu haben zu viele Stufen einen negativen Effekt auf die Transparenz respektive Verständlichkeit.
- **Validierung der konzipierten Rollen durch die verantwortlichen Instanzen**: Diese Instanzen und die Kriterien zur Validierung sind vorab zu definieren. Beispielsweise kann ein sogenannter Role Owner pro konzipierte Rolle definiert werden. Dieser stellt sicher, dass die Rolle funktionstüchtig ist, also alle Einzelberechtigungen beinhaltet, die zwingend notwendig sind. Je nachdem welches Berechtigungsverwaltungssystem Sie schlussendlich verwenden, kann ein solcher Role Owner auch als Genehmigungsinstanz für Rollenantragsprozesse eingebunden werden.
- **Definitionen zur Handhabung des Rollenlebenszyklus'**: Da sich die Gegebenheiten und Aufgaben in Ihrem Unternehmen verändern, sind ggf. auch die implementierten Rollen periodisch zu ändern. Um die notwendigen Arbeiten zeitnah wahrzunehmen, sind bspw. die Zeitintervalle zwischen Rezertifizierungen der Rollen selbst und deren Vergabe zu definieren.

Fazit: Die Anforderungen werden anspruchsvoller – rechtzeitig vorbeugen lohnt sich

Anforderungen an die Sicherheit, Compliance und 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 Verständnis dafür, was eine gute Rollenmodellierung ausmacht und wie man vorzugehen hat, 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:

- Transparenz über die aktuellen Berechtigungsvergaben
- Vorrausetzung für automatisiertes Vergeben oder Entziehen von Rollen, bspw. bei Ein- und Austritten von Mitarbeitenden
- Einhaltung der IT-Governance & Compliance
- Einsparen von Administrationsaufwänden
- Potential für eine Effizienzsteigerung der Geschäftsprozesse

Autor

Thomas Fluri, Business Analyst

Weitere Informationen

www.wib.ch

Thomas Fluri, Business Analyst, WiB Solutions AG