Leitfaden
SAP-Berechtigungen

Dieses Dokument dient der Wissensvermittlung von allgemeinem SAP-Know-how und erhebt keinen Anspruch auf Vollständigkeit oder Richtigkeit. Es basiert auf SAP-Dokumentationen, dem Wissen unserer Mitarbeiter und unseren Projekterfahrungen.

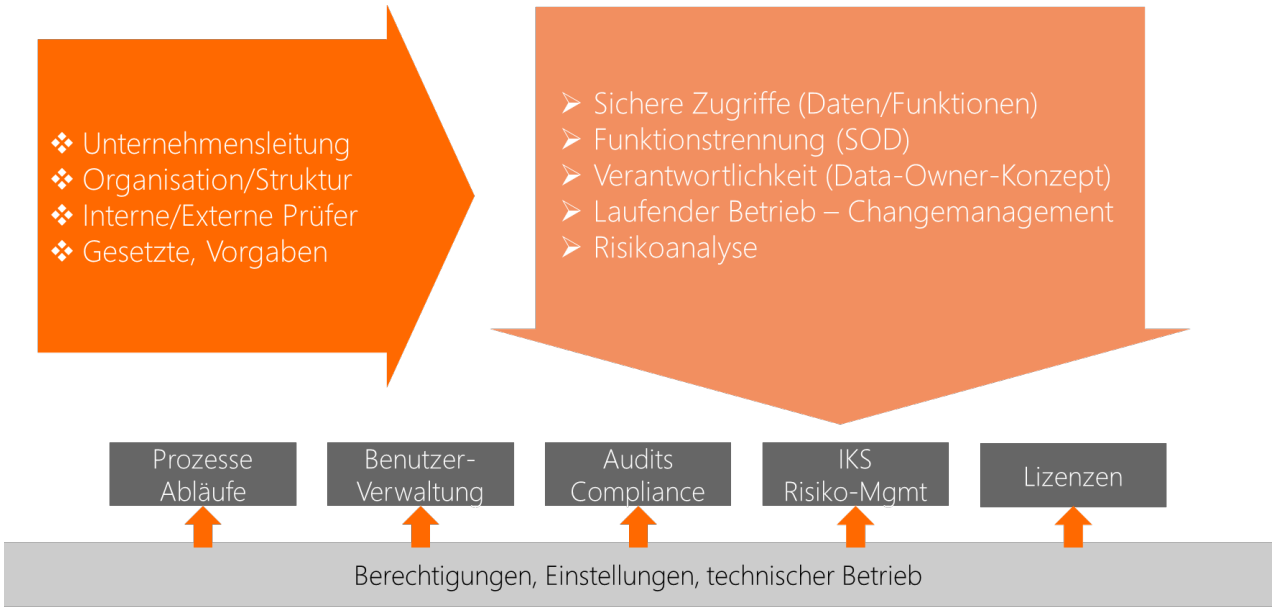
Falls Sie Fehler entdecken, Fragen haben oder Feedback geben möchten, senden Sie bitte eine Mitteilung an support@all-for-one.com. Vielen Dank.

All for One Switzerland AG | Bionstrasse 5 | CH-9015 St. Gallen
fon +41 (0) 58 255 74 00 | info.ch@all-for-one.com | www.all-for-one.ch
Ein Unternehmen der All for One Group SE

Inhaltsverzeichnis

1. Einführung

Ein Berechtigungskonzept hat verschiedensten Anspruchsgruppen zu dienen. Diese stellen Anforderungen oder Rahmenbedingungen, welche in einem Berechtigungskonzept Fragen zu Datensicherheiten, Funktionstrennungen, Verantwortlichkeiten, etc. beantworten. Das Berechtigungskonzept regelt mit diesen Vorgaben den Betrieb und Unterhalt des Systems und bietet Hilfestellungen zu Prozessen, Benutzerverwaltung, Audits oder auch Kontrollen im Rahmen des IKS.



2. Planung von SAP-Berechtigungen

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator, Leiter IT

2.1. Erklärung der wichtigsten Begriffe

Berechtigungen in einem SAP-System steuern die Zugriffsmöglichkeiten seiner Benutzer. Die Sicherheit der Geschäftsdaten hängt daher direkt von den eingestellten Berechtigungen ab. Aus diesem Grund muss die Vergabe von Berechtigungen sorgfältig geplant und durchgeführt werden, um die gewünschte Sicherheit zu erreichen.

Die **Funktionen** eines SAP-Systems (z. B. Programme oder Reports, generell Applikationen im SAP-System) werden über Transaktionen aufgerufen, die dabei unterschiedliche Operationen oder Aktivitäten (z. B. Schreiben, Lesen, Löschen) auf Daten ausführen können. Die über Transaktionen gestarteten Applikationen prüfen beim Aufruf, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen.

Der **Prüfmechanismus** baut auf so genannten Berechtigungsobjekten auf, die Autorisierungsfelder besitzen. Eine konkrete Berechtigung kann als Ausprägung eines Berechtigungsobjektes mit ausgefüllten Autorisierungsfeldern verstanden werden. Beim Start einer Transaktion prüft der SAP-Kern zunächst, ob der Benutzer die Berechtigung zum Start der Transaktion besitzt. Nach dem Start kann die Transaktion auch weitere Berechtigungsprüfungen durchführen. Geprüft wird, ob der zugreifende Benutzer eine Berechtigung besitzt, die vom benötigten Berechtigungsobjekt abgeleitet ist. Ist dies der Fall, werden die Autorisierungsfelder der Berechtigung daraufhin geprüft, ob sie die benötigten Werte oder Wertekombinationen enthalten. Eine Transaktion kann dabei auf mehrere Berechtigungen prüfen. Welche dies sind, wird im Programm-Code festgelegt. Beim Start einer Transaktion wird vom SAP-Kern immer auf das Berechtigungsobjekt S_TCODE geprüft. Beim Start von Applikationen wird auf das Berechtigungsobjekt S_PROGRAM geprüft. Die eigentliche Prüfung erfolgt also immer durch den Kern des SAP-Systems, auch wenn diese durch den Programm-Code der Transaktion angestossen wird.

Fiori Applikationen bauen auf einem Mehrschichten-Prinzip auf. Im Fiori Launchpad (Front End) werden die Applikationen zur Berechtigung in Katalogen (Berechtigung analog Transaktionsstart) geordnet und mittels Gruppen im Launchpad als Kacheln dargestellt. In der Applikation (Back End) finden danach ebenfalls wie beim klassischen GUI-Berechtigungsobjekt-Prüfungen statt.

Aus Applikationssicht sind insbesondere diejenigen Autorisierungsfelder von Berechtigungsobjekten wichtig, die als so genannte **Organisationsebenen** ausgeprägt werden müssen. Sie berechtigen dann eine Rolle, eine bestimmte Transaktion, beispielsweise für den angegeben Buchungskreis (oftmals eine zusammenhängende Geschäftseinheit eines Unternehmens, z. B. Tochterunternehmen) durchzuführen.

Berechtigungen werden Benutzern dadurch zugeordnet, dass ihnen so genannte **Rollen** zugeordnet werden. Rollen geben an, welche Transaktionen (oder Fiori Applikationen) durch den Benutzer ausgeführt werden sollen, dem eine Rolle zugeordnet wurde. Da jede Transaktion auf bestimmte, durch den Programm-Code festgelegte Berechtigungsobjekte prüft, kann für jede Rolle ein Berechtigungsprofil (d. h. Menge von Berechtigungen) abgeleitet werden, in dem alle Berechtigungsobjekte enthalten sind, die zur Ausführung der Transaktionen generell benötigt werden.

Über **Prüfkennzeichen** für Transaktionen kann gesteuert werden, für welche Berechtigungsobjekte, auf die eine Transaktion prüft, der SAP-Kern tatsächlich eine Prüfung ausführt. Über die Prüfkennzeichen können folglich Berechtigungsobjekte beim Aufruf einer Transaktion von der Prüfung ausgeschlossen werden. In diesem Fall wird durch den Profilgenerator auch keine Berechtigung im generierten Berechtigungsprofil erzeugt. Die Prüfkennzeichen werden über die Transaktion SU24 gepflegt, hier werden auch für die einzelnen Autorisierungsfelder der Berechtigungsobjekte die Werte gepflegt, die durch den Profilgenerator in die generierten Berechtigungen der Profile eingetragen werden. Es handelt sich dabei um Vorschlagswerte. Die Profile, die durch den Profilgenerator erzeugt werden, müssen unter Umständen noch manuell nachbearbeitet werden.

SAP unterscheidet verschiedene **Rollentypen**. Einzelrollen beschreiben übergeordnete, von organisatorischen oder anwenderspezifischen Restriktionen unabhängig Funktionen (Bündelung einzelner Arbeitsschritte zu einer Tätigkeit/Aufgabe). Sammelrollen sind die Zusammenfassung von Einzelrollen zu Businessrollen (Funktionsbeschrieb). Berechtigungsrollen haben vom Typ her nur die Funktions- und Datenberechtigungen, enthalten aber keine Menüstruktur, wogegen Menürollen (oder Transaktionsrollen) nur das sichtbare Menü (oder im Fiori Launchpad die Kachelgruppen) enthalten.

2.2. Planungsschritte bei der Vergabe von Berechtigungen

Die Vergabe von Berechtigungen in einem SAP-System ist also ein mehrstufiger Prozess. Zunächst müssen die benötigten (Business-) Rollen definiert werden. Wichtig ist dabei, dass die Rollen letztendlich Arbeitsplätze oder Positionen im Unternehmen beschreiben, diese Rollen haben eine sehr enge Vergleichbarkeit mit Funktionsbeschreibungen. Sie sollten nicht auf einzelne Mitarbeiter bezogen sein, sonst wird die Anzahl an Rollen unübersichtlich und unbeherrschbar. Ein gutes Berechtigungskonzept steht und fällt damit, ob die definierten Rollen sorgfältig spezifiziert wurden.

Die Definition der Business-Rollen muss durch das Unternehmen selbst erfolgen und kann nicht durch den Beratungspartner übernommen werden.

Beispiel einer Rollenmatrix ► sollte durch das Unternehmen erstellt werden

Rollenmatrix
Businessrolle zu Systemrolle

process partner
Service Provider Excellence

Business Rolle	Accountant	Human Resources Professional	Invoicing Central	SAP Admin	Teamlead / Management
Mitarbeiterbeispiel	Thomas Muster	Peter Muster	Maria Muster	Urs Muster	Egon Muster
Aufgabe / Systemrolle					
Basis Rolle	X	X	X	X	X
Zeiterfassung Mitarbeiter	X	X	X	X	X
Zeiterfassung Vorgesetzter					X
User Administration				X	
Rechnungswesen - Experte	X				
Rechnungswesen - Group Reporting	X			X	X
Controlling – Experte	X				
Controlling - Sachbearbeiter			X		
Human Resources - Experte	X	X		X	
Invoicing Sachbearbeiter	*Readonly		X		
Import Schnittstellen	X	X	X	X	

Mögliche Umsetzung: Business Rolle ⏩ Sammelrolle
Aufgabe ⏩ Einzelrolle

Abbildung 1: Beispiel einer Rollenmatrix

Die Definition, ob und wie Einzel- und Sammelrollen, Menü- und/oder Berechtigungsrollen verwendet werden, muss gut überlegt sein, im Berechtigungskonzept dokumentiert und anschliessend systemweit einheitlich verwendet werden.

Sind die Rollen definiert, müssen die zugehörigen Berechtigungsprofile durch den Profilgenerator erzeugt werden. Der Umfang der erzeugten Berechtigungen in den Rollenprofilen wird durch die Konfiguration der Prüfkennzeichen beeinflusst. Auch dies muss sorgfältig geplant werden, da abgeschaltete Prüfungen immer auch einen gewissen Grad an Sicherheitsverlust bedeuten. Die erzeugten Profile und enthaltenen Berechtigungen sind zu prüfen und gegebenenfalls anzupassen.

Bei dieser Aufgabe kann der Beratungspartner unterstützend tätig sein.

Abschliessend werden die Berechtigungen Benutzern dadurch zugewiesen, dass einem Benutzer eine oder mehrere Rollen zugeordnet und der so genannte Benutzerabgleich angestossen wird. Dadurch werden im Benutzerstammsatz die im Berechtigungsprofil der Rolle enthaltenen Berechtigungen gespeichert. Diese Aufgabe obliegt wiederum vollständig den verantwortlichen Mitarbeitern im Unternehmen.

Benutzer-Rollenmatrix

Benutzer zu (mehreren) Business Rollen / Systemrollen

Benutzername	Vollständiger Name	Funktion	Ben. Gruppe	Benutzertyp	Basis Rolle	Zeiterfassung Mitarbeiter	Zeiterfassung Vorgesetzter	User Administration	Rechnungswesen - Experte	Rechnungswesen - Group Reporting	Controlling – Experte
THMUSTER	Thomas Muster	Accountant	FI/CO	A Dialog	X	X	X		X	*Readonly	X
MAMEIER	Max Meier	Human Resources Professional	HR_ADM	A Dialog					X		X
MAMEIER	Max Meier	Accountant	HR_ADM	A Dialog	X	X	X		X	*Readonly	X
MAMUSTER	Maria Muster	Invoicing Central	SD	A Dialog				X		X	X

Abbildung 2: Beispiel einer Benutzer-Rollenmatrix

2.3. Berechtigungskonzept

Das Berechtigungskonzept für ein SAP-System muss je nach Komplexität in einer oder zwei Ausprägungen erstellt werden.

- immer zwingend für den ABAP –Stack — SAP ERP System / Module basierend ABAP
- optional für den Java-Stack — SAP Portal / Funktionen auf Basis Java 2EE

Es gilt dabei zu beachten, dass sich das Berechtigungssystem des SAP-Portals (Java-Stack) fundamental von dem des SAP ERP (ABAP-Stack) unterscheidet. Konzeptionell sind jedoch die gleichen Fragestellungen zu betrachten. Das sind unter anderem:

- Welche Rollen werden benötigt? Sind diese im Einklang mit der Ablauf- und Aufbauorganisation?
- Welche Rolle darf welche Funktionen des SAP-Systems aufrufen (z. B. Transaktionen, Programme, Reports oder Fiori Applications)?
- Welche Rolle darf auf welche Daten des SAP-Systems zugreifen?
- Welche administrativen Rollen mit welchen Berechtigungen werden benötigt, um das geplante Administrationskonzept umzusetzen?
- Nutzen Applikationen neben dem SAP-Standardberechtigungssystem noch weitere Berechtigungen? Diese sind entsprechend im Konzept zu berücksichtigen und zu planen.
- Welche Prozesse für die Berechtigungsverwaltung sind mit den zugehörigen Verantwortlichkeiten zu definieren (z. B. Beantragung, Genehmigung, Anlegen, Verändern, Löschen)?
- Sind Funktionstrennungsaspekte im Berechtigungskonzept ausreichend beachtet? Hier spielen insbesondere auch rechtliche Anforderungen oder Vorgaben eines IKS eine Rolle.
- Was sind die sicherheitsrelevanten Vorgaben bezüglich Login-Verfahren (z.B. Passwortrichtlinien, Audit-Log)?
- Wird das Prinzip eine Notfallusers benötigt und wie sehen die organisatorischen und technischen Prozesse (Antrag, Logging) aus?
- Wird beim Änderungsmanagement auch das Risikopotential betrachtet, welches durch eine Berechtigungshäufung entstehen kann?

Es ist darauf zu achten, dass für alle anfallenden Vorgänge im Kontext von Berechtigungen Prozesse definiert werden und die Prozesse vollständig spezifiziert sind. Zusätzlich sind die jeweiligen Verantwortlichkeiten vollständig festzulegen. So wird verhindert, dass sich durch unklare Verantwortlichkeiten oder unvollständig definierte Prozesse Sicherheitslücken einschleichen.

Die Definition der Rollen und der zugeordneten Berechtigungen muss sich einerseits an den Erfordernissen der Institution orientieren, andererseits müssen hier auch die Anforderungen einbezogen werden, die sich aus den rechtlichen Rahmenbedingungen ergeben. Eine ausführliche Planung ist daher unumgänglich. Je detaillierter die Erfordernisse der Rollen bekannt sind, desto besser können später die Berechtigungen vergeben werden. Dabei ist auf die notwendige Trennung zwischen Rollen zu achten. Es ist empfehlenswert, die Rollen, und damit die Berechtigungen, an die interne Organisationshierarchie und die darin existierenden Positionen und Stellen anzupassen. So kann beispielsweise erreicht werden, dass bei Positionswechseln von Mitarbeitern deren alte Berechtigungen nicht mehr verfügbar sind.

Wichtig ist ausserdem, dass im Unternehmen Verantwortliche für Informationen und Prozesse ernannt werden (Informationseigentümer bzw. Verfahrensverantwortliche), die einen bestimmten Datenbestand der Organisation verantworten. Beispielsweise ist der Leiter der Finanzabteilung (Chief Financial Officer, CFO) für den Finanz- und Controlling Bereich verantwortlich.

Die Verantwortlichen aller Bereiche sind unbedingt in die Planung der benötigten Rollen, Berechtigungen und Prozesse einzubeziehen, da nur sie die dazu notwendigen Kenntnisse auf fachlicher Ebene besitzen. Administratoren sind in der Regel nicht in der Lage, die Rollen und Berechtigungen auf Applikationsebene allein zu planen.

Im Rahmen der Berechtigungsplanung ist auch Folgendes festzulegen

- Welche Berechtigungen sind als kritisch zu betrachten (d. h. erlauben kritische Operationen im SAP-System unter administrativen, rechtlichen oder betriebswirtschaftlichen Aspekten)?
- Welche Rollen dürfen welche kritischen Berechtigungen, Profile oder Rollen erhalten?
- Welche Rollen dürfen welche Werte für kritische Berechtigungsfelder erhalten?

Im Detail unterscheiden sich die Konzepte für den ABAP- und Java-Stack sehr. Für den ABAP-Stack muss die Berechtigungsverwaltung über den Profilgenerator und nicht manuell erfolgen. Generell muss von der manuellen Verwaltung dringend abgeraten werden, da dies häufig zu Fehlkonfigurationen der Berechtigungen führt. Durch den Profilgenerator wird sichergestellt, dass die Benutzer nur die Berechtigungen erhalten, die zum Ausführen derjenigen Transaktionen notwendig sind, die ihnen über die Rollen zugeordnet wurden. Daher ist wichtig, dass insbesondere die Konzepte, Prozesse und Abläufe auf die Verwendung des Profilgenerators abgestimmt sind.

Für den JAVA-Stack besteht hingegen keine Wahlmöglichkeit, da der Berechtigungsmechanismus der Spezifikation der Java 2 Enterprise Edition (J2EE) genutzt werden muss. Es ist dabei zu beachten, dass die «User Management Engine» (UME) über diesen Standard hinausgehende Optionen anbietet.

Es empfiehlt sich, das Berechtigungskonzept in mehreren Dokumenten aufzuteilen. So sollte ein Berechtigungskonzept die oben aufgeführten grundsätzlichen Fragen klären. Dazu gehören nebst den Vorgaben und Prozessen auch Namenskonventionen (Rollen, Benutzer). Mindestens folgende Unterteilung ist sehr zu empfehlen:

- Berechtigungskonzept Grundlagen; wird einmalig erstellt und nur bei wesentlichen Änderungen im Unternehmen oder Vorgaben von aussen (Gesetz, IKS) angepasst

- Berechtigungsmatrix; Auflistung der Businessrollen mit Zuteilung Businessfunktionen (im Einklang mit SAP-Rollen). Dieses Dokument unterliegt einer kontinuierlichen Pflege.

2.4. Planen der Berechtigungsverwaltung

Die Verwaltung der Berechtigungen muss geplant und das gewünschte Verwaltungskonzept muss definiert werden. Im Wesentlichen ist dabei zu berücksichtigen, welche Aufgaben in der Berechtigungsverwaltung durch wen erledigt werden. Hier empfiehlt sich ein rollenbasierter Ansatz, so dass den definierten Rollen später konkrete Benutzer und damit Personen zugeordnet werden können. Dabei ist zu beachten, dass unvereinbare Rollen (Funktionstrennung) nicht derselben Person zugeordnet werden. Da in einer Organisation auch für die Berechtigungsverwaltung schon eine Vielzahl an Rollen impliziert sind, müssen diese entsprechend abgebildet werden.

So gibt es beispielsweise in der Regel keine einzelne Administrator-Rolle, vielmehr sind Rollen wie Benutzer-Administrator, Rollen-Administrator, Berechtigungs-Administrator, Entwickler, Helpdesk-Mitarbeiter oder Transport-Manager zu betrachten. Folglich sind die von SAP vordefinierten Rollen in der Regel nicht ohne Anpassungen zu benutzen.

Prüffragen zum Thema «Planung»

1. Sind die Rollen und Berechtigungen im SAP-System adäquat geplant worden?
2. Werden die vom Profilgenerator erzeugten Profile und enthaltenen Berechtigungen im SAP-System geprüft und gegebenenfalls angepasst?
3. Wird das Berechtigungskonzept im «ABAP –Stack» und «Java-Stack» gleichwertig umgesetzt?
4. Wird darauf geachtet, dass für alle anfallenden Vorgänge im Kontext von SAP-Berechtigungen die Prozesse definiert und vollständig spezifiziert werden?
5. Ist die Verwaltung der Berechtigungen im SAP-System mit allen Prozessen geplant und wurden die Verantwortlichkeiten vollständig definiert?

3. Berechtigungsverwaltung

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator

Die Sicherheit der in einem SAP-System verarbeiteten Geschäftsdaten wird sehr stark durch die eingestellten Berechtigungen für Benutzer und Administratoren bestimmt. Diese legen fest, welche Funktionen (im SAP-Jargon auch Transaktionen oder neu auch Fiori Applications genannt) von einem bestimmten Benutzer aufgerufen und damit, welche Daten eingesehen bzw. verändert werden können. Daher sind die konfigurierten Berechtigungen und deren Verwaltung ein sehr wichtiger Bestandteil der Systemsicherheit, vor allem vor dem Hintergrund möglicher Betrugshandlungen oder auch unbewussten Datenmutationen durch interne Mitarbeiter.

Das SAP-Berechtigungssystem ist sehr flexibel, dadurch aber auch komplex in der Konfiguration. Im Gegensatz zu Betriebssystemen, in denen Berechtigungen direkt auf Objekten (z. B. Dateien) vergeben werden, arbeiten SAP-Systeme nach dem Ausweisprinzip: Beim Zugriff auf Funktionen wird geprüft, ob der Benutzer Berechtigungen eines bestimmten Typs besitzt. Ist dies der Fall, wird geprüft, ob die eingetragenen Werte den Anforderungen entsprechen, die zum Ausführen der aufgerufenen Funktion notwendig sind. Die geprüften Berechtigungstypen und Werte werden dabei durch den Programmierer der Funktion bestimmt und können auch die Daten berücksichtigen, die beim aktuellen Aufruf an die Funktion übergeben wurden. Zusätzlich entscheidet zum Schluss der Programmierer einer Funktion, ob er eine eigentlich notwendige Berechtigungsprüfung implementiert oder nicht. Grundsätzlich arbeitet das SAP-Berechtigungssystem nur im Einschluss-Prinzip, eine Möglichkeit gewisse Funktionen oder Daten auszuschliessen ist nicht möglich.

Für die Verwaltung von Berechtigungen sollten die folgenden Empfehlungen berücksichtigt werden. Die Liste ist an die lokalen Bedürfnisse und Anforderungen anzupassen und zu erweitern.

3.1. Ausbildung

Administratoren, die für die Verwaltung von Benutzerkennungen, Rollen, Profilen oder Berechtigungen verantwortlich sind, müssen zwingend Schulungen zum SAP-Berechtigungskonzept und zur Berechtigungsverwaltung (Vorgehen, Werkzeuge, richtige Verwendung) erhalten oder das entsprechende Verständnis nachweisen. Mit der Einführung des Fiori Launchpad muss zusätzliches Know-how zur Verwaltung von Kacheln aufgebaut werden – speziell ist die Unterscheidung zwischen Katalogen und Gruppen zu erwähnen. Nur so wird erreicht, dass die Berechtigungsverwaltung versiert durchgeführt werden kann.

3.2. Verantwortlichkeiten (Vier-Augen-Prinzip)

Das Benutzerverwaltungskonzept sollte so ausgelegt sein, dass die Verantwortlichkeiten der Berechtigungsverwaltung möglichst **getrennt** werden. Je nach Rolle werden diese in Einführungsprojekten, Change-Projekten, Funktionalitäts-Anpassungen oder im laufenden Betrieb genutzt. Üblicherweise werden im laufenden Betrieb keine Rollen- und Berechtigungsprofile angepasst, sondern müssen über Change-Projekte sauber abgewickelt werden.

- Es sollte ein **Benutzeradministrator** vorgesehen werden. Dieser sollte Benutzerkennungen anlegen, verändern und Rollen zuordnen können. Das Anlegen oder Verändern von Rollen oder Profilen darf dem Administrator nicht erlaubt sein.
  ► SAP bietet hierzu die Vorlage **SAP_ADM_US** (Rolle: SAP_BC_USER_ADMIN)
  ► Zuordnung zur Benutzergruppe **SUPER**

  ☑ Nutzung im Einführungsprojekt
  ☐ Nutzung in Change-Projekten oder Funktionalitäts-Anpassungen
  ☑ Nutzung im laufenden Betrieb

- Es sollte ein **Rollenadministrator** vorgesehen werden, der Rollen anlegen und verändern kann, der jedoch keine Benutzer oder Profile anlegen oder verändern darf.
  ► SAP bietet hierzu die Vorlage **SAP_ADM_AU**
  ► Zuordnung zur Benutzergruppe **SUPER**

  ☑ Nutzung im Einführungsprojekt
  ☑ Nutzung in Change-Projekten oder Funktionalitäts-Anpassungen
  ☐ Nutzung im laufenden Betrieb

- Es sollte ein **Profiladministrator** vorgesehen werden. Dieser darf für vorhandene Rollen Profile generieren, die keine kritischen Systemberechtigungen enthalten (etwa S_USER*), da diese zur Benutzer- und Rollenverwaltung berechtigen.
  ► SAP bietet hierzu die Vorlage **SAP_ADM_PR**
  ► Zuordnung zur Benutzergruppe **SUPER**

  ☑ Nutzung im Einführungsprojekt
  ☑ Nutzung in Change-Projekten oder Funktionalitäts-Anpassungen
  ☐ Nutzung im laufenden Betrieb

- Es sollte ein **Administrator-Administrator** definiert werden. Dieser verwaltet die Benutzer-, Rollen-, und Profil-Administratoren, welche der Benutzergruppe SUPER zugeordnet sind.
  Dieser Benutzer sollte nur im **Vier-Augen-Prinzip** genutzt werden. Er kann beispielsweise durch den Benutzer-Administrator gesperrt und bei Bedarf für die Dauer der Nutzung entsperrt werden.
  ► SAP-Standard – Profil **S_A.SYSTEM**
  ► Zuordnung zur Benutzergruppe **SUPER_ADMIN**

  ☑ Nutzung im Einführungsprojekt
  ☑ Nutzung in Change-Projekten oder Funktionalitäts-Anpassungen
  ☐ Nutzung im laufenden Betrieb

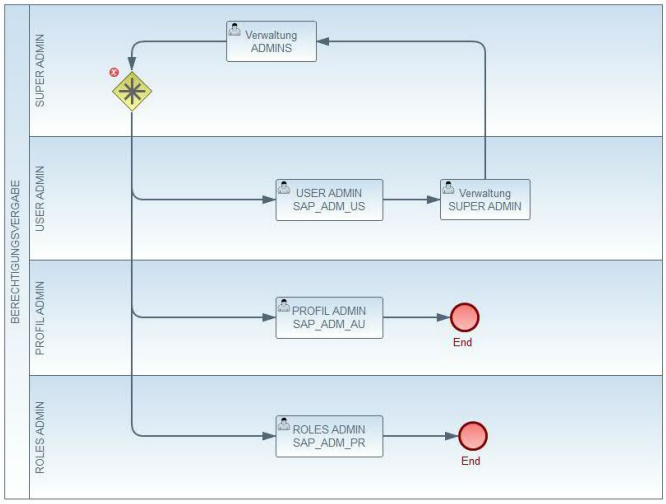


Abbildung 3: Umsetzung des Vier-Augen-Prinzip

Durch die Trennung (sofern technisch richtig umgesetzt) wird erreicht, dass sich die Administratoren nicht selbst Berechtigungen zuordnen können und für sie auf diese Weise nur die ihnen zugeordneten Aufgaben ausführbar sind.

In «kleineren» Unternehmen kann es aufgrund eingeschränkter Personalverfügbarkeit vorkommen, dass keine Trennung vorgenommen werden kann und alle Aufgaben durch eine Person ausgeführt werden. Ebenso ist die Aufgabe der Verwaltung von Berechtigungsprofilen und Berechtigungsdaten verwandt und können bei Bedarf zusammengefasst werden. Alle Daten im SAP-System können dann durch den Administrator unbemerkt eingesehen und verändert werden. Generell ist dies als sicherheitskritisch zu bewerten, so dass zusätzliche Kontrollen notwendig sind. Gleiches gilt allgemein auch im Kontext wichtiger finanz- und bilanzrelevanter Prozesse sowie bei der Verarbeitung personenbezogener Daten, wo beispielsweise eine entsprechende Funktionstrennung vorhanden sein muss. Kann diese nicht erreicht werden, müssen geeignete Kontrollen auf organisatorischer Ebene definiert und deren Durchführung sichergestellt werden. Entsprechende Prüfungen auf das Vorhandensein von Kontrollen finden beispielsweise auch im Kontext von «Sarbanes Oxley Act» bezogenen Prüfungen statt.

Die von SAP vorgegebenen und ausgelieferten Rollen sind sorgfältig gegen die eigenen Anforderungen zu prüfen und anzupassen. Weitere Informationen finden sich in der SAP-Dokumentation unter dem Begriff «Benutzer- und Berechtigungsadministratoren einrichten».

3.3. Prozess der Berechtigungsvergabe

Die Vergabe von Berechtigungen sollte von einer zentralen Stelle koordiniert werden, dem sogenannten «Privileges Manager». Idealerweise ist diese Stelle im HCM-Umfeld angesiedelt, da die Vergabe von Berechtigungen immer in sehr engem Zusammenhang mit der dem Benutzer zugeordneten Business-Rolle steht und diese wiederum von der Position des Benutzers in der Aufbauorganisation abhängt.

Sämtliche Anfragen im Zusammenhang mit der Vergabe von Berechtigungen müssen zentral über diese Stelle laufen, wie z.B.

- Erstellung eines neuen Benutzers
- Änderung/Löschung eines bestehenden Benutzers

- Erstellung und Änderung von Rollen
- Sperren/Entsperren von Benutzern
- Setzen von Gültigkeit eines Benutzers
- Änderung Zuordnung von Rollen und Profilen zu Benutzern (inhaltlich und zeitlich)
- Änderung der Berechtigungen und Generierung von Profilen (Profilgenerator)
- Temporäre Stellvertretungen
- . . .

Um dem definierten Vier-Augen-Prinzip gerecht zu werden, soll die Durchführung dieser Anforderungen jedoch in Abhängigkeit der zu erledigenden Aufgaben durch die folgenden drei Rollen erfolgen.

- Benutzerverwalter (USER ADMIN), HCM- oder IT-Mitarbeiter

- Rollenverwalter (ROLES ADMIN), HCM- oder IT-Mitarbeiter
- Profilverwalter (PROFIL ADMIN), SAP-CC Mitarbeiter oder Berater

Der «Privileges Manager» entscheidet in Abhängigkeit der Anfrage, welche Rolle diese Anfrage erledigen kann, und übergibt diese Aufgabe der entsprechenden Rolle. Er führt ein konsequentes Journal über sämtliche Anfragen und alle durchgeführten Mutationen und Definitionen. Zudem ist er für die Kommunikation zum Anfragesteller bei Rückfragen und Statusmeldungen zuständig.

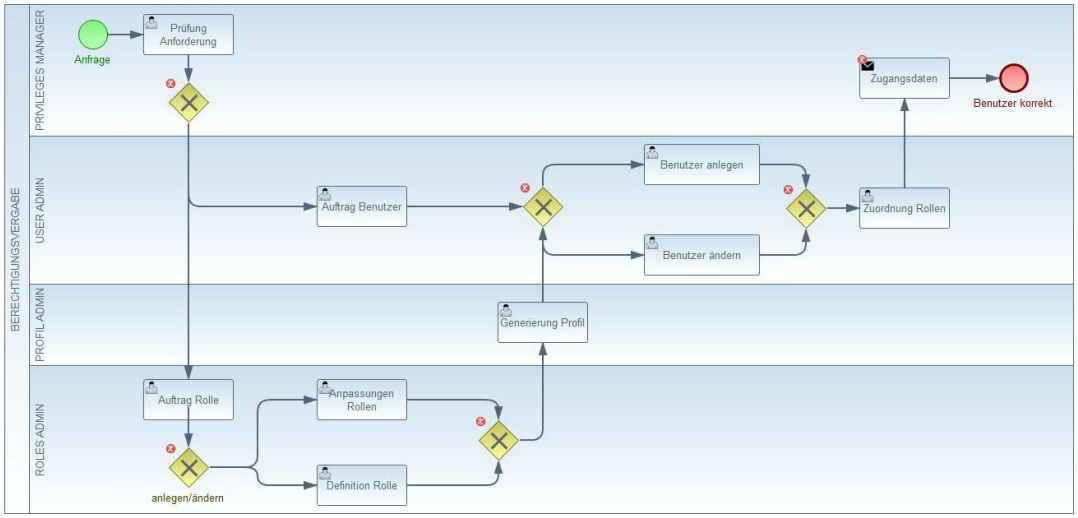


Abbildung 4: Prozess der Berechtigungsvergabe

In einem optimalen Prozess verfügt der «Privileges Manager» nicht über die Berechtigung, diese Aktivitäten selbst durchzuführen, sondern agiert lediglich als Auftraggeber. Bei Kleinunternehmen ist davon auszugehen, dass der «Privileges Manager» und der «SUPER ADMIN» in Personalunion wahrgenommen werden. Dabei kann der «SUPER ADMIN» die anderen Administratoren berechtigen, der «USER ADMIN» kann jedoch den «SUPER ADMIN» in kritischen Situationen sperren.

3.4. Werkzeuge zur Berechtigungsverwaltung

Berechtigungen, Profile und Rollen können auch manuell verwaltet werden. Von diesem Vorgehen wird jedoch aus Sicherheitsgründen dringend abgeraten, da aufgrund der zu verwaltenden Objektmengen bei

manueller Pflege immer Berechtigungsprobleme entstehen. Der Einsatz des Profilgenerators (Transaktion PFCG) wird daher dringend empfohlen. Insbesondere dürfen dann keine manuellen Veränderungen an den Profilen erfolgen.

Administratoren müssen sich mit den Mechanismen und Verfahren beim Einsatz des Profilgenerators vertraut machen, damit eine korrekte Berechtigungsvergabe erfolgt. So muss beispielsweise der Profilgenerator zunächst über die Transaktion SU25 initialisiert werden. Insbesondere die Verwendung und Pflege von Prüfkennzeichen (Transaktion SU24) muss bekannt sein.
In Testläufen können fehlende Berechtigungen (diese sind beispielsweise über die Transaktion SU53 oder über einen Berechtigungstrace mit ST01 feststellbar) erkannt werden.

Neben den systeminternen Werkzeugen zur Berechtigungsverwaltung werden von Drittherstellern auch externe Werkzeuge zur Benutzer- und Berechtigungsverwaltung angeboten. Diese sind in der Regel mit einer komfortableren Benutzungsschnittstelle ausgestattet, da diese direkt auf dem Betriebssystem ablaufen. Ob solche Werkzeuge als Alternative zu den systeminternen Werkzeugen genutzt werden, ist jeweils im Einzelfall unter Kosten/Nutzen-Aspekten zu entscheiden.

3.5. Applikationsspezifische Berechtigungsverwaltung

Einige Produkte und Applikationen nutzen zusätzlich zum SAP-Standardberechtigungskonzept auch noch eigene Berechtigungskonzepte und -verwaltungswerkzeuge (z. B. das «SAP Customer Relationship Management (CRM)» oder das Modul «SAP Human Capital Management (HCM)». Auch die von der All for One Switzerland AG ausgelieferten Lösungen (z.B. ProTime, ProGress) haben ergänzende interne Berechtigungsverwaltungen, welche über eigene Customizing-Werkzeuge beeinflusst werden können.
Dies ist bei der Verwaltung auch zu berücksichtigen, da zusätzliche Verwaltungsschritte und -arbeiten notwendig sind. Insbesondere muss bedacht werden, dass das Produkt oder die Applikation nur dann sicher betrieben werden kann, wenn auch die applikationsspezifischen Berechtigungen über die applikationsspezifischen Verwaltungswerkzeuge sicher konfiguriert wurden. Generell ist dabei auch auf minimale Berechtigungen, Rollentrennung und auf Trennung von Aufgaben und Verantwortlichkeiten zu achten. So darf beispielsweise in einem CRM-System ein Warenbestellkorb nicht durch die gleiche Person zur Bestellung freigegeben werden, die den Warenkorb erzeugt hat.

Generell spielt auf Applikationsebene das Thema Geschäftsrisikomanagement eine wichtige Rolle. Bei der Vergabe von Berechtigungen definiert unter anderem auch das Risikomanagement die Kriterien für die Vergabe von Berechtigungen.

Prüffragen zum Thema «Berechtigungsverwaltung»

1. Existiert ein Rollenkonzept zur Verwaltung des SAP-Systems?
2. Wurden die von SAP vorgegebenen und ausgelieferten Rollen gegen die eigenen Anforderungen geprüft und angepasst?
3. Sind die SAP-Administratoren mit den Mechanismen und Verfahren beim Einsatz des SAP-Profilgenerators vertraut?
4. Wurden die Produktspezifischen Ergänzungen der Berechtigungsverwaltungen erkannt und in die Verwaltung und Prozesse integriert?
5. Wurde berücksichtigt, dass Rollen und Berechtigungsprofile üblicherweise im laufenden Betrieb nicht angepasst, sondern über Change-Projekte abgewickelt werden?

4. Sicherer Umgang mit kritischen SAP-Berechtigungen

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator

Berechtigungen, die im Sinne der Sicherheit oder aus rechtlicher oder betriebswirtschaftlicher Sicht kritische Operationen erlauben, werden von SAP «kritische Berechtigungen» genannt. Betroffen sind z. B. Operationen, die zu Betrug führen können oder über die wichtigen Daten und Konfigurationen gelesen oder modifiziert werden können.

Die Vergabe von kritischen SAP-Berechtigungen muss generell mit besonderer Sorgfalt erfolgen. Der Umgang mit kritischen SAP-Berechtigungen ist daher im Vorfeld zu planen. Organisatorische und technische Massnahmen sowie Prozesse müssen dann sicherstellen, dass das gewünschte Sicherheitsniveau umgesetzt wird. Im Folgenden wird bewusst keine Liste mit kritischen SAP-Berechtigungen angegeben, da diese immer unvollständig wäre und damit Administratoren in falscher Sicherheit wiegt. In der Regel wird dann darauf verzichtet, die Liste zu prüfen und zu erweitern. Die Identifikation kritischer SAP-Berechtigungen für den konkreten Einsatz eines SAP-Systems ist jedoch ein wichtiger Schritt, der auf jeden Fall durchgeführt werden muss.

4.1. Kritische SAP-Berechtigungen, Profile, Rollen identifizieren

Kritische SAP-Berechtigungen hängen aufgrund des SAP-Berechtigungskonzeptes auch von den Feldern und Feldwerten von Berechtigungsobjekten ab. Dies gilt insbesondere für Berechtigungen, die in Applikationen oder Modulen zum Einsatz kommen und damit aus betriebswirtschaftlicher Sicht als kritisch zu betrachten sind. Es wird daher empfohlen, kritische Felder in Berechtigungsobjekten zu identifizieren, um so die betroffenen Berechtigungsobjekte zu identifizieren. Nur so kann eine spätere Prüfung erfolgen, und nur bei Kenntnis der Berechtigungsobjekte kann die Prüfung automatisiert werden. Beispiele für kritische Felder in Berechtigungsobjekten sind Felder für Kostenstellen, Buchungskreis, Profitcenter oder Werk.

Kritische SAP-Berechtigungen sind auch alle Berechtigungen, die im Rahmen der SAP-System-Administration verwendet werden. Dies sind alle Berechtigungen, die von Berechtigungsobjekten abgeleitet sind und mit dem Präfix «S_» beginnen.

Neben Berechtigungen lassen sich auch kritische Profile und Rollen identifizieren, die bereits im Auslieferungszustand enthalten sind. Alle Profile, die auf «_ALL» enden, sind als kritisch anzusehen, da damit in der Regel alle Berechtigungen erteilt werden, die für einen Teilbereich im System, einer Applikation oder eines Moduls relevant sind. Alle Rollen, die die Zeichenkette «ADM» enthalten, sind als kritisch anzusehen, da diese in der Regel administrative Rollen bezeichnen.

Bei der Identifikation kritischer SAP-Berechtigungen, Profile und Rollen ist zu bedenken, dass SAP für Namen zwar ein Konzept vorschlägt, dies aber durch Applikationen oder eigene Entwicklungen nicht immer berücksichtigt wird. Daher können auch kritische Berechtigungen, Profile und Rollen bestehen, die nicht in das vorgenannte Namensschema passen.

Manuell ist die Identifikation kritischer SAP-Berechtigungen insgesamt schwierig. Es sind jedoch von SAP und Drittherstellern Werkzeuge verfügbar, die automatisiert auf kritische Berechtigungen prüfen können. Dabei sind die kritischen SAP-Berechtigungen in der Regel durch den Hersteller der Prüfsoftware vordefiniert.

4.2. Anpassen kritischer SAP-Berechtigungen, Profile, Rollen

Sind die kritischen SAP- Berechtigungen, Profile und Rollen identifiziert, so sollten diese gemäss der Berechtigungsplanung angepasst werden. Insbesondere bei der Anpassung von Profilen und Rollen zur Systemverwaltung müssen die damit verbundenen Effekte für Systemfunktionen berücksichtigt werden. Nach der Anpassung ist daher zu prüfen, ob das gewünschte Systemverhalten erreicht wurde oder ob es zu Fehlfunktionen kommt. Dieser Anpassungsprozess kann bei stärkeren Veränderungen an den vorgegebenen Berechtigungen, Profilen oder Rollen aufwendig und zeitintensiv sein und darf nicht im Produktivsystem durchgeführt werden.

4.3. Verwendung kritischer SAP-Systemberechtigungen einschränken

Im Rahmen der Berechtigungsplanung müssen die Regeln für den Umgang mit kritischen SAP-Berechtigungen, Profilen und Rollen festgelegt werden. Folgende Empfehlungen sind dabei zu berücksichtigen:

Die Profile SAP_ALL, SAP_NEW* und S_DEVELOP* dürfen in einem Produktivsystem nicht genutzt werden. Administrative Berechtigungen, Profile und Rollen dürfen entsprechend der Berechtigungsplanung nur an administrative Benutzer vergeben werden. Auf ausreichende Rollentrennung ist dabei zu achten.

4.4. Liste mit kritischen SAP-Berechtigungen pflegen

Sind die kritischen SAP-Berechtigungen identifiziert, so empfiehlt es sich, diese Liste im SAP-System zu pflegen. Dann kann automatisiert geprüft werden, welchen Benutzern kritische SAP-Berechtigungen zugeordnet wurden. Die Pflege der Liste kritischer SAP-Berechtigungen erfolgt über die Transaktion SU96.

Auch bestimmte Kombinationen von unkritischen SAP-Berechtigungen können kritisch sein, da sie beispielsweise in der Kombination ermöglichen, dass eine oder mehrere als kritisch eingestufte Transaktionen aufgerufen werden können. Ein SAP-System bietet hier die Möglichkeit an, automatisiert nach Benutzern zu suchen, die die Berechtigungen besitzen, bestimmte Kombinationen von Transaktionen aufzurufen. Dazu ist über die Transaktion SU98 (Pflege der Tabelle SUKRI) eine Liste der kritischen Kombinationen zu pflegen.

Mit Hilfe des Report RSUSR008_009_NEW, der die Funktionen der veralteten Reports RSUSR008 und RSUSR009 ersetzt, können Benutzer mit kritischen Berechtigungen und mit kritischen Kombinationen von Berechtigungen ermittelt werden.

Die im Auslieferungszustand eines SAP-Systems enthaltenen Listen für die kritischen SAP-Berechtigungen und Transaktionskombinationen sind nur als Beispiel anzusehen und sollten nicht für die Überprüfungen

genutzt werden. Die Listen müssen selbst aufgebaut und gepflegt werden. Diese können beispielsweise auch bei «Sarbanes Oxley Act» bezogenen Prüfungen begutachtet werden.

In diesem Kontext bietet SAP für die NetWeaver-Plattform mit dem «SAP GRC Access Control» kostenpflichtig ein entsprechendes Zusatz-Prüfwerkzeug an, so dass entsprechende Risiken automatisiert erkannt werden können. Prüfwerkzeuge sind auch von Drittherstellern erhältlich.

Prüffragen zum Thema «Kritische Berechtigungen»

1. Sind die kritischen SAP-Berechtigungen, Profile und Rollen identifiziert und gemäss der Berechtigungsplanung angepasst?
2. Werden Tabellen mit kritischen SAP-Berechtigungen und kritischen Kombinationen von Transaktionen im SAP-System gepflegt?

5. Konfiguration zusätzlicher SAP-Berechtigungsprüfungen

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator

Ein SAP-System erlaubt es, die vorkonfigurierten Berechtigungsprüfungen zu verändern. Berechtigungsprüfungen können deaktiviert werden. Es können auch zusätzliche Berechtigungsprüfungen erfolgen. Im Rahmen der Berechtigungsplanung ist diese Möglichkeit zu berücksichtigen. Generell ist bei Veränderungen an den Berechtigungsprüfungen Folgendes zu bedenken:

5.1. Deaktivieren von Berechtigungsprüfungen

Werden vorhandene Berechtigungsprüfungen deaktiviert, so kann dies die Sicherheit des SAP-Systems gefährden, da damit Zugriffskontrollen abgeschaltet werden. Bevor Prüfungen deaktiviert werden, müssen die Auswirkungen auf die Sicherheit sorgfältig geprüft werden.

5.2. Erzeugen von Transaktionen für den Start von Programmen oder Reports

Programme und Reports können beispielsweise über die Transaktion SE38 oder SE80 (ABAP Editor) gestartet werden. Nicht jedem Programm oder Report ist jedoch ein Transaktionscode zugeordnet. Sollen bestimmte Programme oder Reports Benutzern verfügbar gemacht werden, so empfiehlt sich, diese über eine Transaktion verfügbar zu machen. Dies hat den Vorteil, dass der Zugriff auf die Transaktion und damit das Programm oder den Report über Berechtigungen vom Typ S_TCODE geschützt werden können. Zusätzlich kann der Zugriff auf die Transaktionen SE38 und SE80 gesperrt werden, da damit prinzipiell beliebiger Code ausgeführt werden kann.

Auch bei diesem Vorgehen ist zu beachten, dass weiterhin die durch den Profilgenerator erzeugten Berechtigungen zum Aufruf von Programmen oder Reports gepflegt werden müssen. Dazu sind die vom Berechtigungsobjekt S_PROGRAM abgeleiteten Berechtigungen in den Rollen-Berechtigungsprofilen entsprechend der Berechtigungsplanung zu modifizieren.

5.3. Einsatz von Parametertransaktionen

Über neu angelegte Parametertransaktionen können für Transaktionen Werte oder Wertebereiche für die Aufrufparameter vorgegeben werden. Die neu angelegten Parametertransaktionen (Transaktion SU93) können dann über eigene Berechtigungen (Berechtigungsobjekt S_TCODE) zugriffsbeschränkt werden.

Es ist in diesem Zusammenhang wichtig zu berücksichtigen, dass der Einsatz von Parametertransaktionen nicht als Sicherheitsverfahren geeignet ist, um den Zugriff auf Funktionen der Transaktion oder auf Daten zu beschränken. Generell muss der Zugriff, beispielsweise auf Programme, Reports oder Tabellen, immer über die entsprechenden Berechtigungsobjekte (S_PROGRAM für Programme und Reports, S_TABU_DIS für Tabellen) eingeschränkt werden.

5.4. Anpassen der ABAP-Berechtigungsgruppen

Für Programme, Reports und Tabellen können sogenannte Berechtigungsgruppen definiert werden. Damit kann eine Gruppierung erfolgen, so dass der Zugriff auf die Programme, Reports oder Tabellen einer Gruppe über ein Berechtigungsobjekt gesteuert werden kann.

5.5. Einsatz von ABAP-Berechtigungsgruppen

Folgendes ist beim Einsatz von ABAP-Berechtigungsgruppen zu beachten.

- Der Zugriff wird immer auf alle Objekte einer Gruppe reglementiert.
- Die Berechtigungsgruppe stellt eine zusätzliche Prüfung dar. Die normalen Berechtigungsprüfungen, die das Programm oder der Report durchführt, werden davon nicht berührt.
- Werden Berechtigungsgruppen genutzt, so kann in der Planung mit einer groben Gruppierung, etwa bezüglich einzelner Applikationen oder Module, begonnen werden. Diese können dann entsprechend dem gewünschten Schutzbedarf weiter verfeinert werden.
- Die genaue Funktionsweise von Berechtigungsgruppen und deren Verwaltung muss Planern und durchführenden Administratoren bekannt sein.

5.6. Eigene zusätzliche Berechtigungsobjekte

Werden im Unternehmen oder der Behörde eigene (ABAP-) Programme, CDS-Views oder Fiori Applications entwickelt oder der Programmcode vorhandener Programme modifiziert, so können auch Berechtigungsprüfungen für neue, selbst definierte Berechtigungsobjekte eingebaut werden. Damit diese durch den Profilgenerator berücksichtigt werden, müssen die Prüfkennzeichen über die Transaktion SU24 definiert und entsprechend angepasst werden. Dies ist im Rahmen der «Change-Management – Prozesse» umzusetzen.

5.7. Veränderungen dokumentieren

Alle Veränderungen an der Berechtigungsprüfung sind zu dokumentieren.

Prüffragen zum Thema «Zusätzliche SAP-Berechtigungsprüfungen»

1. Werden SAP-Berechtigungsprüfungen nur nach sorgfältiger Prüfung deaktiviert?
2. Werden die durch den SAP-Profilgenerator erzeugten Berechtigungen zum Aufruf von Programmen oder Reports entsprechend der Berechtigungsplanung gepflegt?
3. Sind die genaue Funktionsweise von SAP-Berechtigungsgruppen und deren Verwaltung den Planern und durchführenden Administratoren bekannt?
4. Wurden für eigene Entwicklungen oder Modifikationen die Auswirkungen auf die Berechtigungen berücksichtigt?

6. Regelmässige Sicherheitsprüfungen

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator, IT-Sicherheitsbeauftragter, Revisor

Die Sicherheit eines SAP-Systems kann nur dann auf Dauer gewährleistet werden, wenn dieses regelmässig geprüft wird. Auf diese Weise können Fehlkonfigurationen und Schwachstellen aufgedeckt und behoben werden.

Sicherheitsprüfungen sollten in regelmässigen Abständen durch unterschiedliche Personen erfolgen. So sollten beispielsweise Administratoren in relativ kurzen Abständen (etwa monatlich) Kurzprüfungen durchführen. Es empfiehlt sich dabei, eine Prüfliste aufzubauen, damit ein definierter Prüfumfang gewährleistet ist. Festgestellte kleinere Probleme können meist sofort durch die Administratoren korrigiert werden, grössere Probleme sind entsprechend der Prozessvorgaben weiter zu melden. In mittleren Zeitabständen (mehrere Monate) sollten Sicherheitsprüfungen durch andere, interne Rollen (z. B. Informationssicherheit, IT-Revision) erfolgen. In längeren Zeitabständen können dann auch Prüfungen durch externe Prüfer sinnvoll sein.

Folgende Aspekte sind bei Prüfungen zu berücksichtigen:

6.1. Regelmässige Recherche von sicherheitsrelevanten Informationen

Generell müssen sich Administratoren und für die Informationssicherheit verantwortliche Personen regelmässig über Neuerungen und Änderungen informieren, die die verantworteten Systeme betreffen. Dazu sind insbesondere die SAP-Informationsquellen regelmässig zu sichten.

6.2. Berechtigungen für Revisionsbenutzer

Für das SAP-Benutzerkonto, das zur Prüfung der Systemkonfiguration durch externe Personen genutzt wird, sollten nur lesende Berechtigungen vergeben sein. Veränderungen dürfen durch den Revisionsbenutzer nicht durchgeführt werden. Im ABAP-Stack darf dem Revisionsbenutzer nicht das Profil SAP_ALL zugeordnet werden.

Können die Berechtigungen des Revisionsbenutzers nicht auf den lesenden Zugriff beschränkt werden, so darf der Zugriff nur im Vier-Augen-Prinzip erfolgen.

SAP bietet ein eigenes «Audit System (Audit Information System, AIS)» an, das es Revisoren ermöglicht, ein SAP-System zu untersuchen. Dabei sind bereits unterschiedliche Rollen und Berechtigungen verfügbar, die dem Benutzerkonto des Revisionsbenutzers zugeordnet werden können. Die verfügbaren Rollen sind in der Regel so gestaltet, dass nur lesender Zugriff besteht. Die Rollen können im Profilgenerator (Transaktion PFCG) über die Suche «SAP*AUDITOR*» eingesehen werden.

6.3. Zugriff auf AIS konfigurieren

Für die Prüfung kann das «Audit Information System (AIS)» eingesetzt werden. Das AIS liegt in unterschiedlichen Versionen vor.

- als Transaktion SECR und
- in der rollenbasierten Version

Über die Transaktion SECR können Prüfungen teilweise automatisiert erfolgen. Das AIS erlaubt es ausserdem, das Prüfergebnis zu dokumentieren und den Prüfstatus (Ampel-Status: rot, gelb, grün) vorzuhalten.

Es empfiehlt sich, eine Untermenge der angebotenen Prüfmöglichkeiten zu definieren (Top 10 Security Reports) und diese abzuarbeiten. Dabei ist die festgestellte Ist-Konfiguration gegen die Soll-Konfiguration zu prüfen.

Es ist zu bedenken, dass das AIS kritische Systeminformationen preisgibt. Der Zugriff muss daher auf die berechtigten Prüfer eingeschränkt werden (S_TCODE, Transaktion SECR).

Im Gegensatz zur Transaktion SECR besteht das rollenbasierte AIS aus vorgefertigten Rollen, Berechtigungen und Programmen, die es ermöglichen, einem Benutzer die für ein Audit notwendigen Berechtigungen auf System- und Modul-Ebene zu erteilen. Im Fokus stehen dabei vornehmlich kaufmännische Audits. Das rollenbasierte AIS muss entsprechend eingerichtet und konfiguriert werden.

6.4. Prüfen der Veränderungen der Systemänderbarkeit

Die Einstellungen zur Systemveränderbarkeit sind regelmässig zu prüfen. Dazu kann die Transaktion «SE03 Administration / Systemänderbarkeit» genutzt werden. Zu prüfen sind die globalen Einstellungen und die Einstellungen für jeden Mandanten.

Für den Java-Stack besteht nicht die Möglichkeit, die Systemänderbarkeit durch Systemeinstellungen zu konfigurieren.

6.5. Security Auditlog

Das «Security Auditlog» enthält sicherheitsrelevante Protokolleinträge. Eine regelmässige Auswertung muss daher erfolgen. Für die Auswertung können die Transaktionen SM20, SM20N oder RZ27_SECURITY eingesetzt werden, wobei die Transaktion SM20N aufgrund der besseren Benutzungsschnittstelle zu bevorzugen ist. Um die Transaktionen SM20 und SM20N verwenden zu können, muss vorher mit der Transaktion SM19 der Auswerteumfang definiert und das Auditlog aktiviert werden.

6.6. Profilparameter

Die eingestellten Profilparameter sind gegen die geplanten Soll-Werte zu prüfen. Die gültigen Profilparameter lassen sich auch direkt über die Transaktion SM20N anzeigen. Alternativ kann der Report RSPARAM über die Transaktion SE38 ausgeführt werden.

6.7. Benutzerinformationssystem

Über das Benutzerinformationssystem (Transaktion SUIM) sollten regelmässig Prüfungen erfolgen. Folgende Informationen sind dabei sicherheitsrelevant.

- Benutzer mit Falschanmeldungen
  ► dies kann auf Angriffsversuche hindeuten
- Benutzer mit Anmeldedaten und Kennwortänderungen
  ► So lassen sich Benutzer identifizieren, die nie angemeldet sind oder ihr Passwort nicht geändert haben, sofern dies nicht automatisch erzwungen wird
- Benutzer mit kritischen Kombinationen von Berechtigungen für den Transaktionsstart
  ► es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen
- Benutzer mit kritischen Berechtigungen
  ► es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen
- Änderungsbelege für Benutzer, Rollenzuordnungen, Rollen, Profile und Berechtigungen
  ► hierbei ist insbesondere auf Änderungen an administrativen Objekten zu prüfen
- Erreichbare SAP-Gateways

Über die Transaktion RSGWLST können die von einem SAP-System erreichbaren SAP-Gateways anderer SAP-Systeme bestimmt werden. Dies zeigt die Verbindungs- und Zugriffsmöglichkeiten auf. Es können die Einstellungen der Datei «secinfo» der entfernten Gateways eingesehen werden, über die die Autorisierungen zum Ansprechen und Registrieren des entfernten SAP-Gateways definiert werden. Zusätzlich können die Destinationen und die registrierten RFC-Server-Programme der ansprechbaren entfernten SAP-Gateways abgeprüft werden.

Die Auswertung erfordert jedoch entsprechende technische Kenntnisse. Da über die Transaktion RSGWLST auch sensitive Systeminformationen erlangt werden können, muss die Transaktion zugriffsbeschränkt werden.

Der Status des SAP-Gateways des lokalen Systems kann über die Transaktion SMGW (Gateway Monitor) geprüft werden.

6.8. Prüfen der Single Sign-On (SSO) Möglichkeiten

Benutzer können sich an einem SAP-System zunächst mit gültigen Authentisierungsinformationen (z. B. Benutzername/Passwort, Zertifikat) anmelden und dann über den SSO-Mechanismus ohne erneute Eingabe von Authentisierungsinformationen auf andere SAP-Systeme zugreifen.

Über die Transaktion STRUST können die Zertifikate anderer SAP-Systeme eingesehen werden, die das lokale SAP-System bei SSO-Zugriffen akzeptiert. Hier sollten nur vertrauenswürdige Systeme eingetragen sein. Alternativ kann die Prüfung auch über die Transaktionen SSO2 oder SSO2_ADMIN erfolgen.

6.9. Regelmässige Prüfung der Berechtigungen

Das vollständige Prüfen von Berechtigungen ist in der Regel aufgrund des Mengengerüstes nicht manuell möglich. Daher ist ein gutes Berechtigungskonzept unbedingt notwendig. Aber auch dann müssen die Berechtigungen regelmässig auf Konsistenz mit dem Berechtigungskonzept geprüft werden. Hier können Stichproben (siehe auch «Benutzerinformationssystem» oben) für wichtige Benutzergruppen durchgeführt werden. Das Berechtigungskonzept muss sicherstellen, dass Prozesse aufgesetzt sind, die verhindern, dass Berechtigungen angesammelt werden.

Zusätzlich können Werkzeuge zum Einsatz kommen, die ein integriertes Änderungs- und Risikomanagement anbieten, so dass beispielsweise die Möglichkeit des Betrugs durch Benutzer aufgrund von Berechtigungsproblemen verringert werden kann. SAP bietet dazu den so genannten «SAP GRC Access Control» an, der die konfigurierten Berechtigungen dahingehend prüft, ob Benutzer Berechtigungen besitzen, die aus Sicherheitssicht als kritisch zu betrachten sind. Solche Prüfungen finden typischerweise auch im «Sarbanes-Oxley»-Umfeld statt, sind generell jedoch für jedes Unternehmen sinnvoll. Die Prüfung muss die unter diesen Gesichtspunkten kritischen Berechtigungen für Transaktionen (wie etwa SE80, SE16, SQVI oder kritische Autorisierungsobjekte für Benutzer, beispielsweise S_PROGRAM, S_USER_GRP, S_TABU_DIS, S_RFC, S_USR_RFC) erkennen und anzeigen. Ähnliche Prüfwerkzeuge sind auch von Drittherstellern erhältlich.

6.10. Aktualität der Updates prüfen

Für das SAP-System ist die Aktualität der installierten Updates zu prüfen. Dazu kann die Transaktion SPAM eingesetzt werden. Der aktuelle Patch-Stand des Systems muss dann mit den verfügbaren Patches verglichen werden. Dies erfordert, dass dem Prüfer die von SAP verfügbaren Patches bekannt sind. Die Prüfung muss auch auf Fehler oder Warnungen bei Updates erfolgen. Dabei ist zu beachten, dass Warnungen auch dann existieren können, wenn der Update-Status auf «grün» steht.

6.11. Sicherheit der Kommunikationsschnittstellen prüfen

Die Sicherheit der unterschiedlichen Kommunikationsschnittstellen sollte geprüft werden. Dies betrifft beispielsweise die RFC-, ICF- und ALE-Schnittstellen des ABAP-Stack und die Schnittstellen des Java-Stacks.

Hier ist insbesondere zu prüfen, wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind.

Prüffragen zum Thema «Regelmässige Sicherheitsprüfungen»

1. Werden im SAP-System in regelmässigen Abständen Sicherheitsprüfungen mit definiertem Prüfumfang durchgeführt?
2. Werden im SAP-System die Einstellungen zur Systemänderbarkeit (globale Einstellungen, Einstellungen für jeden Mandanten) regelmässig geprüft?
3. Erfolgt eine regelmässige Auswertung des «Security Auditlog» im SAP-System?
4. Werden die eingestellten Profilparameter im SAP-System gegen die geplanten Soll-Werte geprüft?
5. Erfolgt im SAP-System regelmässig eine Prüfung zum Benutzerinformationssystem?
6. Werden im SAP-System die Berechtigungen regelmässig auf Konsistenz mit dem Berechtigungskonzept geprüft?
7. Wird für das SAP-System die Aktualität der installierten Updates geprüft?
8. Werden im SAP-System die Kommunikationsschnittstellen (z.B. RFC, ICF und ALE) geprüft, insbesondere wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind?

7. Einschränkung direkte Tabellenveränderungen

Verantwortlich für Initiierung	IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung	Administrator

Alle Daten eines SAP-Systems werden in den Tabellen der Datenbank des SAP-Systems gehalten. Bei der Nutzung erfolgen die Tabellenveränderungen z. B. durch die aufgerufenen Transaktionen, Programme oder RFC-Bausteine.

7.1. Berechtigungen auf Tabellen-Zugriffstransaktionen einschränken

Im SAP-System besteht die Möglichkeit, auch direkt auf die Inhalte von Tabellen lesend oder verändernd zuzugreifen. Der Zugriff auf Tabellen und Tabelleninhalte kann durch unterschiedliche Transaktionen erfolgen, wie z.B. SE16(N) Data Browser, SE80 Workbench, SE84 Repository Browser, SM30 Pflege Tabellensichten, SM31 Pflege Tabellen, SE11 Data Dictionary, SQVI Quick Viewer.

Je nach Version des SAP-Systems und je nachdem, welche Applikationen und Module installiert sind, können auch zusätzliche Transaktionen oder Reports existieren, die direkte Tabellenzugriffe erlauben.

Der Zugriff auf die oben genannten Transaktionen sollte mindestens eingeschränkt werden, so dass nur die berechtigten Administratoren oder Benutzer diese aufrufen können. Die Liste der Transaktionen, die aus diesem Grund zugriffsbeschränkt werden sollten, muss entsprechend der lokalen Systemausprägung erweitert werden. Der Zugriff wird über das Berechtigungsobjekt S_TCODE konfiguriert.

Es wird empfohlen, regelmässig zu prüfen, welche Benutzer auf die in diesem Sinne kritischen Transaktionen zugreifen können. Dazu kann beispielsweise das Benutzerinformationssystem (Transaktion SUIM) genutzt werden, über das Benutzer nach unterschiedlichen Suchkriterien aufgelistet werden können.

Über die Transaktion S_BCE_68001398 können direkt die Benutzer aufgelistet werden, die auf eine bestimmte Transaktion Zugriff besitzen. Diese Transaktion kann für Einzeltests benutzt werden.

7.2. Berechtigungen für den Tabellenzugriff konfigurieren

Können die Transaktionen für den direkten Tabellenzugriff nicht beschränkt werden, so besteht die Möglichkeit, Tabellenzugriffe über direkte Berechtigungen auf Tabellen zu steuern. Die dabei benutzten Berechtigungsobjekte sind S_TABU_DIS, S_TABU_NAM, S_TABU_CLI und S_TABU_LIN. Über das Berechtigungsobjekt S_TABU_DIS können Berechtigungen auf mandantenbezogene Tabellen-Gruppen vergeben werden. Diese werden in der Tabelle TBRG definiert und fassen einzelne Tabellen zu Gruppen zusammen. Für jede Tabellen-Gruppe wird über die Tabelle TDDAT eine zugehörige Berechtigungsgruppe definiert. Für die Zugriffssteuerung werden die Namen der Tabellen-Berechtigungsgruppen als Werte in den Parameter DIBERCLS aufgenommen. Die erlaubten Operationen werden über den Parameter ACTVT gesteuert. Über das Berechtigungsobjekt S_TABU_CLI können analog Berechtigungen auf mandantenunabhängige Tabellen-Gruppen vergeben werden.

Es ist unbedingt notwendig, die Berechtigungsobjekte S_TABU_DIS, S_TABU_NAM und S_TABU_CLI für die Zugriffskontrolle auf Tabellen einzusetzen, wenn der Zugriff auf Transaktionen, die direkten Tabellenzugriff erlauben, nicht ausgeschlossen ist.

Mittels S_TABU_LIN lassen sich Berechtigungen auf einzelne Tabellenzeilen vergeben. Dieser Mechanismus erfordert jedoch zusätzliche Customizing-Einstellungen. Hierzu müssen so genannte Organisationskriterien definiert und aktiviert werden.
Aufgrund der Komplexität der Definition der Autorisierungsreichweiten wird dieses Objekt in der Praxis eher selten verwendet.

Eine häufig genutzte Variante, den Zugriff auf bestimmte Tabellen zuzulassen, ist die Definition von Parametertransaktionen. Dadurch werden Transaktionen definiert, die andere Transaktionen mit vordefinierten Werten aufrufen. Im vorliegenden Fall wird dann die Transaktion SE16(N) direkt mit dem gewünschten Tabellennamen aufgerufen. Der Tabellenname wird dann als Wert für den Parameter «DATABROWSE-TABLENAME» in den Vorschlagswerten definiert. Parametertransaktionen werden über die Transaktion SE93 definiert. Bei diesem Vorgehen ist zu beachten, dass trotzdem die Zugriffsberechtigungen für Tabellen über S_TABU_DIS vergeben werden müssen, da Parametertransaktionen nicht zur Zugriffssteuerung geeignet sind.

Prüffragen zum Thema «Einschränkung direkte Tabellenveränderungen»

1. Haben nur berechtigte SAP-Administratoren oder SAP-Benutzer direkten Zugriff auf Tabellentransaktionen?
2. Wird regelmässig überprüft, welche SAP-Benutzer auf kritische Tabellentransaktionen zugreifenkönnen?