Revision 4.0

Christoph Wildensee

Identifizierung der Risiko-Ebenen bei der Berechtigungsprüfung in SAP HCM

1. Vorwort

Nach wie vor ist die Prüfung der Berechtigungssteuerung in SAP HCM komplex, allerdings aufgrund des eigentlich klaren Ergebnishorizontes abgrenzbar. Dies ist umso leichter, wenn das HCM-System als „closed-shop"-System eigenständig gefahren wird und die vergebenen Berechtigungen nicht als Modul-Mischrechte offeriert werden. Grundsätzlich sind hoch privilegierte Berechtigungen nur im Personalbereich auszumachen. Die Abrechnung – ob intern angesiedelt oder über einen externen Dienstleister nach Art. 28 i. V. m. Art. 4 Nr. 10 DSGVO realisiert – und die administrative Personalsachbearbeitung/Referentensicht sind sicherlich die wesentlichen Bereiche mit solchen Rechten, die man in einer Betrachtung erwartet. Abgeschwächt sind auch die Berufsaus- und -weiterbildung (ausdrücklich auf Daten für Zwecke der Ausbildungsförderung und -verwaltung) und der Betriebsrat zu nennen, die regelmäßig Sichtzugriff auf sensible Informationen der Beschäftigten erhalten können. Doch ist zunächst vor einer Berechtigungsanalyse zu hinterfragen, was eigentlich eindeutig sensible und vor allem dahingehend abgrenzende Informationen sind.

Nach Tabelle T778T können mehrere hundert Infotypen, die als Informationsabgrenzung und Datenqualifizierer gelten, innerhalb der zuständigen P-Berechtigungsobjekte herangezogen werden, um mit verschiedenem Manipulationsgrad eine Fachbereichsrolle auszuprägen.

Während Personen aus der Führungsebene einige Informationen zu den nach Stellenplan bzw. Über-Unter-Ordnungsverhältnis ihnen zugewiesenen Beschäftigten im Zugriff erhalten dürfen und es hier leider kaum eine für alle Unternehmen und Hierarchiestufen ableitbare Regel geben kann, die einen solchen Zugriff im Detail klarstellt, sieht dies ausdrücklich bei **Sichtzugriffen auf Gehaltsbestandteile** anders aus. Insbesondere die **Infotypen 0008** (Basisbezüge) und **0015** (Ergänzende Zahlungen/Einmalzahlungen) sind in Deutschland schützenswerte Informationen (vgl. z. B. BAG, Beschluss vom 07.05.2019, Az. 1 ABR 53/17). Auch wenn nach dem Entgelttransparenzgesetz (EntgTranspG, 2017) Auskunftsansprüche existieren, kann es hierfür natürlich im Bedarfsfall nur für ausgewählte Personen des Betriebsrats (als institutionalisierte Arbeitnehmervertretung) ergänzende Rechte außerhalb des Personalbereiches geben. Andere Bereiche und Personen können kaum einen permanenten Einsichtsanspruch ableiten.

Um das Berechtigungskonzept also zu prüfen, ist es zunächst sinnvoll, das Sichtrecht auf die Infotypen 0008 und 0015 für Personen außerhalb der eigenen Person zu analysieren. Dies betrifft die Berechtigungsobjekte P_ORGIN und P_PERNR. Ergänzend kommt für eine Vielzahl von Unternehmen die Steuerungsoption aus dem Objekt P_ORGXX hinzu (erweiterte Berechtigungsprüfung T77S0 → AUTSW → ORGXX 1). Zuletzt müssen auch – ausgehend von der Tabelle USOBT – die Transaktionsebene und alle übrigen, notwendigen Objektausprägungen einbezogen werden. Während in vielen SAP-Bereichen ein fehlendes Recht zum Transaktionsaufruf im Benutzerstammsatz substituiert werden kann durch Transaktionen wie z. B. SA38, OODR, START_REPORT oder ähnliche und der Angabe des hinter der gewünschten Transaktion stehenden Programmnamens, funktioniert diese Vorgehensweise für die Transaktionen PA20 (Personalstammdaten anzeigen) und PA30 (…pflegen) nicht. Insoweit muss eine der beiden Transaktionen in privilegierten Stammsätzen vorkommen, was wiederum eine wesentliche Funktion zur Separierung der Rechte darstellt. Zeigt die vollständige Sicht am Ende als Ergebnis, welche Stammsätze und daraus, welche Bereiche Zugriff erhalten, ist üblicherweise auch die Frage nach der adäquaten Steuerung beantwortet. Unabhängig davon ist die Zuweisung der Stellen zu einer Leitungsfunktion (Stelle leitet Anzahl Stellen aus dem Org.Mng.) nicht Inhalt dieser Betrachtung.

Die nachfolgende Zusammenfassung zeigt im Wesentlichen eine mögliche Herangehensweise bei der Analyse der Berechtigungssteuerung in SAP HCM.

2. Prüfungsvorgehen

Sofern wir annehmen, dass das Sichtrecht auf die Infotypen 0008 und 0015 bei anderen Personen als wesentliche Identifier der Rollenwahrnehmung und -trennung und die Transaktion PA20 ebenfalls hierzu dienen kann, bestehen mehrere Schritte zur Eingrenzung der Rollen und Berechtigungen. Der erste Schritt besteht darin, die wesentlichen Arbeitsplatzrollen und deren Zuweisung zu den Stammsätzen zu identifizieren. Hierzu kann zunächst die Tabelle AGR_USERS herangezogen werden. Innerhalb dieser Tabelle stehen sowohl die Einzel- als auch die Arbeitsplatz-/Sammelrollen, die den UserIDs/Stammsätzen mit Gültigkeitsbeginn und -ende zugewiesen sind. Eine Eingrenzung muss sowohl bezüglich der Namensgebung aus der Konvention heraus auf Sammelrollen als auch über FROM_DAT und TO_DAT erfolgen. Sinnvoll ist hier z. B., dass bei TO_DAT ein Datum größer voraussichtliches Prüfungsbeendigungsdatum gewählt wird. Ansonsten können die Ergebnisse eine eingeschränkte Aktualität aufweisen. Zunächst steht für dauerhaft beschäftigte Personen im Feld TO_DAT der 31.12.9999. Bei der Bedeutung der Rollen hilft die Einsicht in die Tabelle AGR_DEFINE mit den Feldnamen AGR_NAME und TEXT.

Tabelle: AGR_USERS
Angezeigte Felder: 11 von 11 Feststehende Führungsspalten: 5 Listbr

MANDT	AGR_NAME	UNAME	FROM_DAT	TO_DAT
000	.H_ABRECHNUNG	H 02	16.12.2009	31.12.9999
000	.H ABRECHNUNG	HD 9	05.12.2003	31.12.9999
000	.H_ BRECHNUNG	HD .5	05.12.2003	31.12.9999
000	.H BRECHNUNG	HG 7	01.01.1900	31.12.9999
000	.HI ABRECHNUNG	HT 9	05.12.2003	31.12.9999
000	.H BRECHNUNG	HT 7	16.12.2009	31.12.9999
000	.HI BRECHNUNG	HT 7	01.08.2017	31.12.2100
000	.H BRECHNUNG	HX 9	01.01.1900	31.12.9999
000	.H BRECHNUNG	SV	05.12.2003	31.12.9999
000	.H BRECHNUNG	UA 43	18.01.2022	31.12.2024

Tab. 1: Inhalte der AGR_USERS.

Liegen diese Inhalte eingegrenzt vor, kann im nächsten Schritt die Tabelle beispielsweise in eine MS Access-Datenbank eingelesen und dort als **Kreuztabelle** dargestellt werden. Nach MS Excel- Transfer kann wiederum diese Rohliste um die weniger wichtigen Rollen reduziert werden. Dadurch erhält man eine **qualifizierte Rollen-User-Stichprobe**, die weitere Inhalte aufnehmen kann. Notwendig ist an dieser Stelle, dass die organisatorische Zuweisung der UserIDs hinzugelesen wird, um Bereichsgruppierungen ableiten zu können. Hierzu dient die Tabelle USER_ADDR. Die Felder „Vollstän-

diger Name“ und „Abteilung“ (Department) sind von großem Vorteil, um die korrekte Bereichszuweisung erkennen und hiernach sortieren zu können.

Welche Arbeitsplatz-/Sammelrollen sind nun relevant?

Sofern eine Einzelrolle eine Eingrenzung des Objektes P_PERNR mit PSIGN=E oder * in der Tabelle AGR_1251 aufweist (Ausschluss = I), kann eine Arbeitsplatzrolle mit einer solchen zugewiesenen Einzelrolle auf Personalnummern zugreifen, die nicht die eigene ist (Zugriff auf die eigene Personalnummer ist für den „Employee Self Service“ [ESS] notwendig: insoweit wird es üblicherweise im Stammsatz ein P_PERNR mit PSIGN=I geben). Erhält man nun eine Liste der Einzelrollen, die P_PERNR im Feld PSIGN=E oder * (nicht I) aufweisen, müssen diese Einzelrollen auf Infotyp 0008 und 0015 überprüft werden. Werden diese in der Tabelle AGR_AGRS als Child geprüft, können die relevanten Arbeitsplatzrollen identifiziert und die Kreuztabelle sinnvoll reduziert werden. Weniger kompliziert ist der Weg über die Transaktion SUIM und der Suche nach „Einzelrollen mit Berechtigungsdaten“ oder „Benutzer nach komplexen Selektionskriterien“.

Final erhält man eine auf die neuralgischen Sammelrollen reduzierte Liste der UserIDs und Bereiche sowie deren Zugriffsauslöser. Weitere Überprüfungen können stichprobenartig bezüglich der sonst notwendigen Objektausprägungen erfolgen. Insbesondere erfolgt die Prüfung des Objektes P_ORGIN auf Infotyp 0008 und 0015 in diesen Rollen (Personalbereiche = T500P; Personalbereiche = T501; Mitarbeiterkreis = T503K). Abschließend erhält man die Liste der relevanten Sammelrollen für die Ergebnisliste.

Tabelle: USOBT
Angezeigte Felder: 9 von 9 Feststehende Führungsspalten: 5 Listbreite 0250

NAME	TYPE	OBJECT	FIELD	LOW	HIGH
PA20	TR	PLOG	INFOTYP	1001	
PA20	TR	PLOG	ISTAT		
PA20	TR	PLOG	OTYPE	C	
PA20	TR	PLOG	OTYPE	O	
PA20	TR	PLOG	OTYPE	P	
PA20	TR	PLOG	OTYPE	Q	
PA20	TR	PLOG	OTYPE	S	
PA20	TR	PLOG	PLVAR	&PLVAR	
PA20	TR	PLOG	PPFCODE		
PA20	TR	PLOG	SUBTYP		
PA20	TR	P_ABAP	COARS		
PA20	TR	P_ABAP	REPID		
PA20	TR	P_ORGIN	AUTHC	R	
PA20	TR	P_ORGIN	INFTY		
PA20	TR	P_ORGIN	PERSA		
PA20	TR	P_ORGIN	PERSG		
PA20	TR	P_ORGIN	PERSK		
PA20	TR	P_ORGIN	SUBTY		
PA20	TR	P_ORGIN	VDSK1		
PA20	TR	P_PCLX	AUTHC	R	
PA20	TR	P_PCLX	RELID	PC	
PA20	TR	P_PCLX	RELID	TX	
PA20	TR	P_PERNR	AUTHC		
PA20	TR	P_PERNR	INFTY		
PA20	TR	P_PERNR	PSIGN		
PA20	TR	P_PERNR	SUBTY		

Tab. 2: Tabelle USOBT zur Transaktion PA20 und den notwendigen Objektausprägungen im Stammsatz.

Besonderheit „Erweitere Berechtigungsprüfung“

Die erweiterte Berechtigungsprüfung über P_ORGXX ist eine zusätzliche Ebene, eine oder sogar mehrere mögliche Berechtigungsprüfungen einzuziehen. Hierbei werden spezifische Profile genutzt, die mit ergänzenden Funktionsbausteinaufrufen erweitert werden können. Für einige Arbeitsplatzfunktionen werden jeweils Profile angelegt, die beim Check des Zugriffes greifen, sofern sie dann zur UserID in Tabelle T77UA (UNAME, PROFL, BEGDA, ENDDA; Erläuterungen hierzu in Tabelle T77PQ) hinterlegt sind. Ist hier kein Profil für eine UserID hinterlegt, und privilegierte Objektausprägungen sind für sie im Stammsatz vorliegend, gibt es nur aus diesen die Einschränkungen. Die Person hat aber auf privilegiert hinterlegte Infotypen aller Beschäftigten (mindestens lesenden) Zugriff.

Beispiel: Erhält ein/e Mitarbeiter/in die Fachbereichsfunktion für die zeitwirtschaftlichen Aufgaben des Bereiches und hat über eine weitere Rolle Zugriff über P_ORGIN auf INFTY 0008/0015 und die Transaktion PA20 inkl. aller für diese Transaktion notwendigen, weiteren Ausprägungen, greift zusätzlich P_ORGXX aus der erweiterten Berechtigungsprüfung im Stammsatz, wenn zu der Funktion ein Profil hinterlegt ist und dieses eine zusätzliche Prüfung aufweist. Ist in dieser Prüfung dann ein begrenzendes Ordnungskriterium hinterlegt, erhält die Person mit PA20 nur Zugriff auf die Personen, die diesem Ordnungskriterium entsprechen. Dies gilt an der Stelle für alle Infotypen.

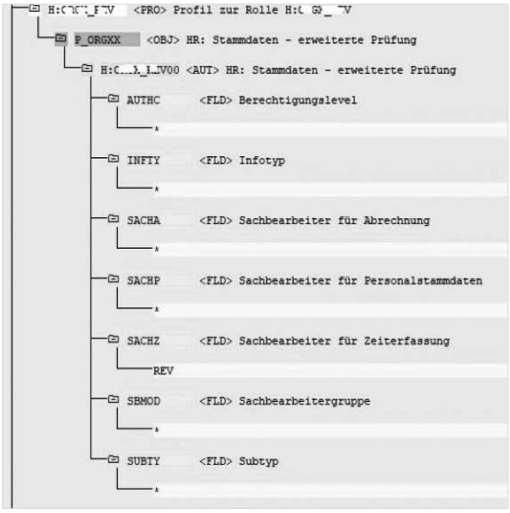


Abb. 1: P_ORGXX-Objekt mit begrenzendem Ordnungskriterium aus dem Bereich Revision.

Die Person im Beispiel kann also nicht auf alle Beschäftigten des Unternehmens mit PA20 zugreifen, sondern nur auf die Personen, die dem Ordnungskriterium REV entsprechen (INFTY und alle anderen Felder bei P_ORGXX = *), dort allerdings auf alle Infotypen, die

unter dem Objekt P_ORGIN angegeben wurden. Auch wenn ein zweites P_ORGXX im Stammsatz vorhanden ist, sucht sich (dies ist ein Unterschied zu SAP Core, hier zählt die höchste Ausprägung im Stammsatz) SAP HCM die Objektausprägung, die mit dem Profil eine Eingrenzung aufweist. Ist dies der Fall, wird auf die Eingrenzung reduziert. Im Beispiel ist die Referenz der pflegenden Personen zum Ordnungskriterium SACHZ in Tabelle T526 zu finden (SACHX, SACHN und USRID).

Wie erfolgt hier die Steuerung?

In der Transaktion OOSB (Benutzer strukturelle Berechtigung) findet sich jeweils je UserID, die z. B. zeitwirtschaftliche Aufgaben übernimmt, ein Eintrag mit einem Profil-Namen und einer Gültigkeit.

Abb. 2: OOSB – Besondere Benutzerberechtigungen.

Lässt man sich die Objekte hierzu zur Person anzeigen, so zeigt sich, dass hier die Personalnummern eingetragen sind, für die diese Person tatsächlich die Aufgabe übernimmt. Eine Person aus einem anderen Bereich kann dann in der Sachbearbeitung der zeitwirtschaftlichen Aufgaben nicht ausgewählt werden. Es werden nur die hier enthaltenen Personen in Gültigkeit angezeigt, die unter ObjektId mit der Personalnummer stehen.

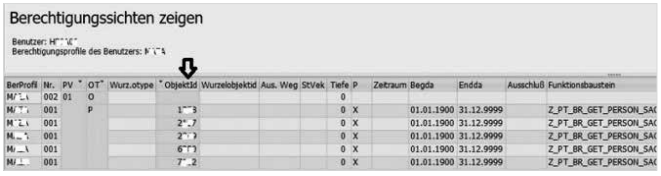


Abb. 3: Zugehörige Datensätze, ObjektId beinhaltet zugehörige Personalnummern und Prüfungs-FuBa.

Zum Profil wird der Ablauf aus dem Funktionsbaustein Z_PT_BR_GET_PERSON_SACHZ mitgegeben, der eine Prüfung auf SACHZ-Ebene durchläuft (FuBa hinterlegt zum Profil der Funktion des Mitarbeiters mit zeitwirtschaftlichen Aufgaben in Tabelle T77PR; Felder PROFL, LFDNR, PLVAR, OTYPE [=P] und PFUNC).

(Auszug aus Report)

```
FUNCTION z_pt_br_get_person_ sachz .
[…]
CALL FUNCTION 'GET_AUTH_VALUES'
    EXPORTING
       object1      = 'P_ORGXX'
       user  = uname
       optimize     = ' '
    TABLES
       values= values
    EXCEPTIONS
       user_doesnt_exist = 1
       OTHERS       = 2
[…]
  LOOP AT values
    WHERE field = 'SACHZ'.
    IF values-von EQ '*'.
      DELETE values.
    ELSE.
      temp_r_sachz -sachz_v = values-von(3).
      temp_r_sachz -sachz_b = values-bis(3).
      COLLECT temp_r_sachz .
    ENDIF.
  ENDLOOP.
[…]
LOOP AT temp_sachz.
    sy-subrc = 0.
    CLEAR pernr_list[].
    SELECT pernr
        INTO CORRESPONDING FIELDS OF
          TABLE pernr_list
        FROM pa0001
        WHERE  sbmod = temp_sachz-sbmod AND
               sachz = temp_sachz-sachz AND
               sprps = space
               AND begda LE sy-datum
               AND endda GE sy-datum .
    SORT pernr_list. "YIK
    DELETE ADJACENT DUPLICATES FROM
      pernr_list COMPARING pernr.
    LOOP AT pernr_list.
      result_tab-otype = 'P '.
      * (siehe Abb., OT=Objekttyp)
      result_tab-objid = pernr_list-pernr.
      COLLECT result_tab.
    ENDLOOP.
  ENDLOOP.
[…]
```

Der vergleichende Referenzwert für den implementierten, zusätzlichen Abgleich steht im Stammsatz der zugewiesenen Beschäftigten im Feld PA0001-SACHZ (Verknüpfung zu T526-SACHX). Ist also ggf. eine weitere Personalnummer versehentlich zugewiesen, die dem Ordnungskriterium nicht entspricht, dann wird der Zugriff abgelehnt – eine doppelte Absicherung nur zulässiger Zuweisungen.

Es ist also wichtig, zuletzt zu den UserIDs mit zeitwirtschaftlichen Aufgaben in der Kreuztabelle/Ergebnisliste die jeweils zugewiesenen Ordnungskriterien hinzuzufügen, um abschätzen zu können, ob die Zugriffe auf alle Beschäftigten des Hauses oder nur auf eine stark begrenzte Gruppe zutreffen und ggf. auch mit weiteren, hoch privilegierten Rechten kombiniert werden. Beschäftigte des Personalbereichs weisen wiederum keine Profile auf, da sie auf alle Beschäftigten des Unternehmens Zugriff erhalten. Zur Übersicht ist hier die Bereichsgruppierung relevant. Sofern Zuständigkeitsaufteilungen innerhalb der Personalbearbeitung notwendig sind, wird hier analog verfahren.

Ähnlich ist auch die Steuerung des Managers Desktop (MD) für Führungskräfte. Es wird allerdings die **WurzelobjektID** als Basis in OOSB genutzt. Hier steht die Stellennummer der Führungskraft. Unter ObjektId stehen die Personalnummern (Objekttyp P) und die Stellennummern (Objekttyp S) der zugewiesenen Personen. Die Stellennummer der WurzelobjektID wird auch in der Tabelle T527X zur jeweiligen Bereichskennung gehalten (ORGEH, BEGDA, ENDDA und ORGTX). Zu den Profilen des Managers Desktop in T77UA gibt es in T77PR aber keine Funktionseinträge, die Prüfungen auf Referenzfelder beinhalten, da dies über die Hinterlegung der Auswertungswege nach T778A ausreicht (Referenz auf SAP-FuBa RH_GET_...). In vielen Unternehmen läuft dieses Procedere annähernd wie dargestellt. Die FuBa-Namen und Prüfungsobjekte sind dann aber abweichend.

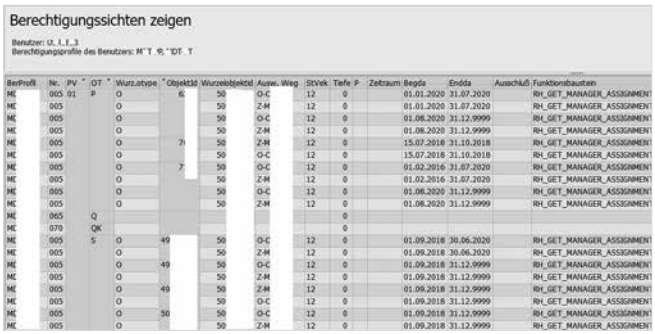


Abb. 4: WurzelobjektId, ObjektId und Objekttyp.

Im Bereich der Rechte auf Managers Desktop weist jede Führungskraft unter T77UA also ein oder mehrere MD-Profile auf, die wiederum keine weitere Eingrenzung aus P_ORGXX benötigen, da der Stellenplan greift, keine Einträge in T77PR vorliegen und sich die MD-Rechte nur auf Personen beziehen, die in der Hierarchiedarstellung analog der Verknüpfung zugeordnet sind. Andere Profile können jedoch ebenfalls eine Referenz auf einen Funktionsbaustein (angepasst im Kundennamensraum) aufweisen.

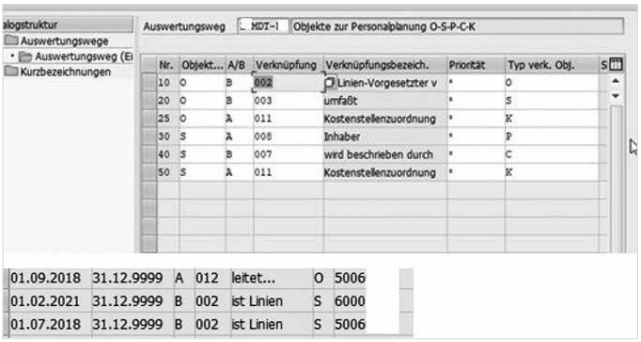


Abb. 5: Über-Unter-Ordnungsverhältnis in HCM.

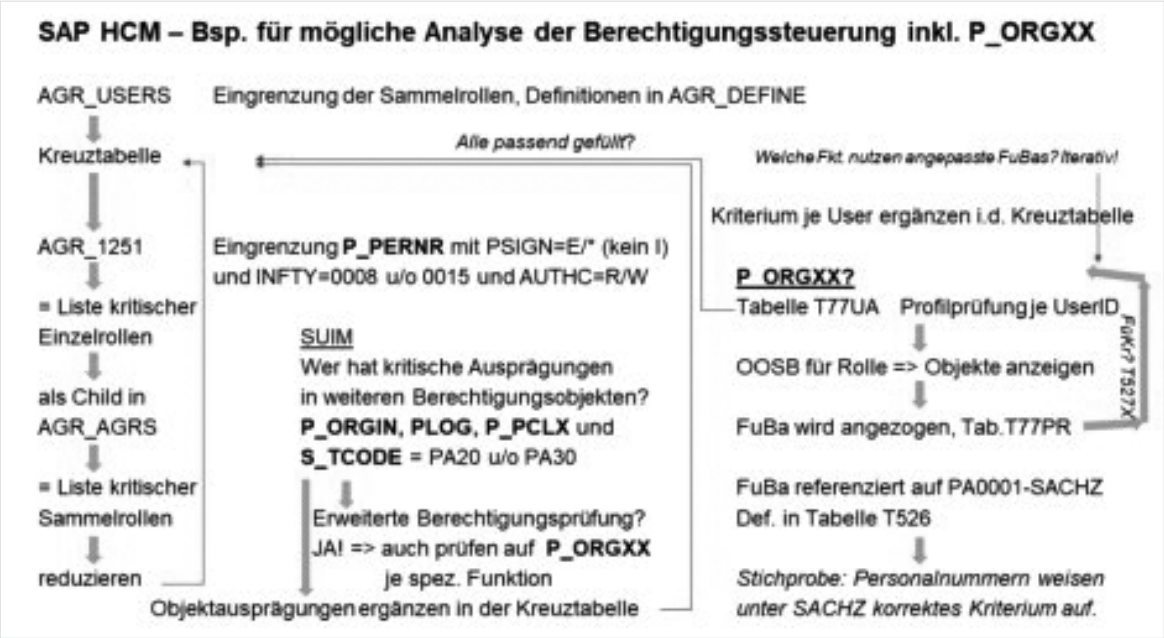
3. Ergebnis/Fazit

Ziel der Analyse ist die Feststellung der kritischen Vergabe (mindestens) lesender Rechte auf Gehaltsbestandteile der Beschäftigten. Dabei sind sowohl die Bereiche/Zuständigkeitsgruppen als auch die Personen zu identifizieren, die einen solchen Zugriff aufweisen, um hieraus Anpassungsbedarf des Rollenmodells abzuleiten. Darüber hinaus können auch die verschiedenen, ergänzenden Berechtigungsprüfungen identifiziert werden, die bei unterschiedlichen Funktionsprofilen gem. Tabelle T77UA und T77PR greifen; denn beliebige Funktionswahrnehmungen im Bereich der Sachbearbeitung der Personaldaten (innerhalb des Personalbereiches wie auch in weiteren Fachbereichen) können über den Aufruf eines Funktionsbausteins mit ergänzenden und beliebig umfassenden Berechtigungsprüfungen oder anderen Code-Abläufen versehen werden. Weitere Profile außerhalb des Personalbereiches sind also durchaus bedeutsam.

Die Nutzung insbesondere der im Kundennamensraum vorliegenden Funktionsbausteine mit ergänzenden Berechtigungsprüfungen, die in Profilen genutzt werden, lässt sich herausfinden über:

Alle Funktionen/FuBa	Alle Funktionen/FuBa zu jedem PROFL
`SELECT T77PR.PFUNC FROM T77PR WHERE T77PR.PROFL IN (SELECT T77UA.PROFL FROM T77UA GROUP BY T77UA.PROFL) GROUP BY T77PR.PFUNC;`	`SELECT T77PR.PFUNC, T77PR.PROFL FROM T77PR WHERE T77PR.PROFL IN (SELECT T77UA.PROFL FROM T77UA GROUP BY T77UA.PROFL) GROUP BY T77PR.PFUNC, T77PR.PROFL;`

Dies ist sinnvoll, da hier die Funktionsübernahme-abweichende Ablaufsteuerung (PROFL) in der Personalsachbearbeitung erkannt werden kann, um auch die DSGVO-Konformität der Berechtigungssteuerung prüfen zu können. Wie viele und welche Funktionsbau-



Anlage 1: Schema-Beispiel.

steine nutzen wir im Unternehmen für eine solche Steuerung? Welche Profile sind mit Kundennamensraum-FuBa für welchen Zweck erweitert worden? Was steht in den FuBas als ergänzende Prüfung/Code-Abläufe und mit welchen Referenzfeldern sind sie verbunden? Die FuBas können über SE37 analysiert werden.

Das finale Ergebnis muss aus dem Personalbereich bestätigt werden, damit das Risiko final akzeptiert wird und die Anpassung dokumentiert ist. Zusätzlich sollten weitere Infotypen-Zugriffe auf Rollenebene und auch auf Leitungsebene (Vorstände/Geschäftsführung und leitende Angestellte) als Prüfungsfokus im Laufe der Zeit zumindest betrachtet werden.

S_TABU_DIS benötigt zusätzlich einen Ausschluss mindestens aller PA-, SA- und SS-Tabellen (Personal-[Zugriff nicht einmal lesend] & Berechtigungstabellen [wenn, dann ausdrücklich nur lesend]), auch S_TABU_NAM sollte auf keine solcher Tabellen explizit berechtigen.

Allerdings werden ggf. vereinzelte Zugriffe auf die Gruppe PA speziell in der Moduladministration benötigt. Die sinnvolle und dabei praktikable Eingrenzung ist ein Balance-Akt. Und schließlich sollten auch Zugriffe über Transaktion SE37 und S_RFC auf die Funktionsgruppen 7004, BPAY und HR_I* im Produktionssystem unterbunden werden, da hiermit das Recht verbunden ist, u.a. unter Angabe einer beliebigen Personalnummer, z.B. mit den Bausteinen BAPI_GET_PAYSLIP, *_HTML und *_PDF, einen Abrechnungsbeleg darzustellen (FuBas teilweise auch remotefähig). Die Gruppe HR_INFOTYPE8_PAYROLL beinhaltet den im Zugriff zu entfernenden Abrechnungssimulationsbaustein HR_PAYROLL_TEST_PAYSLIP_SHOW. Berechtigungsseitig sollten das Produktionssystem und darunterliegende Systeme (Test, Integration etc.) gleichgeschaltet werden.

Insbesondere bei der Rollenvergabe des Personalbereiches/Personalabrechnung und des Betriebsrates ist bei einem Bereichswechsel privilegierter Personen in andere Bereiche, in denen diese Rechte nicht zugestanden werden, die Karenzzeit zum Entzug der Rollen auf 0 Tage zu setzen. Speziell bei Auszubildenden im Vertiefungsjahr, die dieses im Personalbereich absolvieren und dort bereits Sachbearbeitungen aufgrund der zugestandenen Rollen erbringen sollen, besteht das hohe Risiko, dass sie noch über einen längeren Zeitraum die Rechte des Personalbereiches aufweisen, obwohl sie bereits den Personalbereich verlassen und im anderen Bereich Aufgaben übernommen haben.

[Aus stilistischen Gründen bzw. zur Vereinfachung der Lektüre wird häufig die männliche Schreibweise verwendet. Die weibliche Form ist jeweils ebenso gemeint und zu bedenken.]

Dipl.-Betriebswirt Christoph Wildensee, DBA, MFTA, CISM, CRISC, CDPSE, ist seit vielen Jahren in der Internen Revision der enercity AG, Hannover, tätig. Zwischen 2008 und 2012 war er in Personalunion Datenschutzbeauftragter des Unternehmens und der zugehörigen Netzgesellschaft.