Berechtigungsprüfungen in SAP R/3 HR – Personalwirtschaft

Personalwirtschaftliche Vorgänge werden in SAP R/3 im Modul HR – Human Resources – verwaltet. Entsprechend anspruchsvoll gestaltet sich das Datenmodell und die vorhandenen Steuerungs- / Customizing- und Sachbearbeitungsfunktionalitäten. Das Modul HR ist somit der zentrale Bestandteil im SAP-Integrationsmodell bei der Verarbeitung personenbezogener Daten.

Dipl.-Betriebswirt Christoph Wildensee, CISM, ist IV-Revisor bei der Stadtwerke Hannover AG (enercity), einem großen kommunalen Energiedienstleister mit ca. 2.500 Mitarbeitern und mehr als 1 Mrd. EUR Umsatz. Er verfügt über eine langjährige Prüfungserfahrung im Bereich der Revision, er arbeitete projektbezogen auch für die IBS-Gruppe aus Hamburg in der SAP-Beratung und ist Verfasser verschiedener Fachartikel insbesondere zum Thema SAP-Prüfung.

Der aus Sicht der Revision immanenten Gefahr einer unsachgemäßen, ggf. sogar missbräuchlichen Nutzung entsprechender Daten / Information kann nur durch ein adäquat ausgestaltetes Berechtigungskonzept begegnet werden. Nachfolgend wird aufgezeigt, welche Zugriffsschutzmechanismen in HR existieren und welche Möglichkeiten bestehen, für eine angemessene Funktionsversorgung bei gleichzeitiger Transparenz bestehender Berechtigungen zu sorgen.

Das Modul HR umfasst unter anderem die Funktionen [1].

- Organisationsmanagement (als übergreifend-integraler Bestandteil)
- Personalmanagement mit Bereichen wie Personalbeschaffung, -entwicklung und andere
- Personalplanung (Personalbedarfs-, -beschaffungs-, -einsatz-, -entwicklungs- und -kostenplanung zzgl. Vergütungsmanagement)
- Veranstaltungsmanagement
- Reisemanagement
- Personalabrechnung
- Zeitwirtschaft
- Bescheinigungswesen.

Bereits dieser kurze Abriss zeigt deutlich, dass die Verwaltung personenbezogener und damit von Natur aus kritischer Informationsblöcke eine erweiterte Prüfung bedingt – und diese erfolgt über die Berechtigungsobjekte des ’P*’-Bereiches.

Insbesondere die unterschiedlichen Steuerungsfelder und deren mögliche Ausprägungen sind für den Revisor maßgeblich. Während die Generalberechtigung (’*’) grundsätzlich problematisch ist, können Einzelausprägungen ebenfalls kritisch sein.

Mögliche Steuerungswerte können in zwei Gruppen unterschieden werden, die erste Gruppe sind Werte zur Zugriffssteuerung bestimmter Funktionen, d.h. zum Beispiel Reise anlegen, abrechnen, stornieren oder ähnliches, die zweite Gruppe sind Werte zur dezidierten Berechtigung auf bestimmte personenbezogene Daten, d.h. zum Beispiel über die Personalnummer, die Bezeichnung einer Mitarbeitergruppe, die Kennung einer bestimmten Mitarbeiterdatengruppierung (Infotyp).

In den meisten Unternehmen ist es üblich, dass die Sachbearbeitung im Personalbereich eine Unterscheidung in der Betreuung unterschiedlicher Mitarbeitergruppen erhält, z.B. Arbeitnehmer, Rentner, Vorstand / GF, Prokuristen / Leitende Angestellte etc. Insbesondere die Abschottung der hierarchisch höher angesiedelten Mitarbeiter (Bearbeitung nur durch wenige ausgesuchte Mitarbeiter) liegt an der unterschiedlichen Ausgestaltung von Arbeitsverträgen, die bei dieser Gruppe besondere Vertragsbestandteile beinhalten, die nicht jeder einsehen können soll. Eine besondere Beachtung erhalten also Steuerungstabellen, die eine spezielle Sicht auf bestimmte Unternehmens- und Mitarbeitergruppen aus unterschiedlichen Blickwinkeln ermöglichen. Diese sind z.B.

- Personalbereich (Tabelle T500P)
- Personalabrechnungskreis (Tabelle T549A)
- Mitarbeitergruppe (Tabelle T501)
- Mitarbeiterkreis (Tabelle T503K/T503T)
- [Bewerbergruppe (Tabelle T750K)
- Bewerberkreis (Tabelle T750F)] .

Dies sind auch maßgebliche Unterscheidungsmerkmale in den Berechtigungsausprägungen.

Zusätzlich erfolgt eine besondere Unterscheidung relevanter Daten über die Mitarbeiter-datengruppierung (inhaltlich zusammenhängende Attribute), der sog. Infotyp-Steuerung. Infotypen (Informationstypen) gruppieren die Stamm- und Bewegungsdaten der Mitarbeiter analog der Tab. 1, so dass auch dezidierte Berechtigungen auf Teilbereiche der Daten einzelner Mitarbeiter möglich sind. Die nachfolgend dargestellten Infotypen sind die wichtigsten bei der Unterscheidung der Datenblöcke.

Infotyp	**Beschreibung**
0000	Maßnahmen
0001	Org. Zuordnung
0002	Daten zur Person
0003	Abrechnungsstatus
0004	Behinderungen
0005	Urlaubsanspruch
0006	Anschriften
0007	Soll-Arbeitszeit
0008	Basisbezüge
0009	Bankverbindung
0010	Vermögensbildung
0011	Ext. Überweisungen
0012	Steuerdaten
0013	Sozialversicherungsdaten
0014	Wiederkehrende Be-/Abzüge
0015	Ergänzende Zahlungen (Einmalzahlungen)
0016	Vertragsbestandteile
0017	Reiseprivilegien
0021	Familie / Bezugsperson
0022	Ausbildung
0023	Tätigkeiten bei anderen Arbeitgebern
0024	Qualifikationen
0025	Beurteilungen
0026	Direktversicherung
0045	Darlehen (auch Prüfung auf F-Objekte [z.B. Debitor])
0078	Darlehenszahlungen

Infotyp	Beschreibung
0079	Sozialversicherungszusatzversorgung
1000-1999	Organisationsmanagement
2000-2999	Zeitwirtschaft
4000-4999	Bewerbermanagement / Personalbeschaffung
9000-9999	Kundeneigene Erweiterungen

Tab. 1: Ausgesuchte Infotypen

Das Berechtigungskonzept von HR ist bereits sehr umfangreich, aber es ist möglich, im HR-Customizing erweiterte Prüfungen zu aktivieren. Diese werden durch die Ausprägung der Tabelle T77S0 gesteuert. Die unterschiedlichen Steuerungsschalter der Gruppe AUTSW beziehen sich auf die HR-Berechtigungsfunktionen. Nachfolgend wird ein Auszug aus dieser Tabelle gezeigt.

Mandant	Gruppenname	Kürzel	Standardwert	Erklärung
xxx	AUTSW	ADAYS	15 *(Tage)*	HR: Toleranzzeit der Berechtigungsprüfung
xxx	AUTSW	APPRO	0 *(keine Pr.)*	HR: Prüfverfahren
xxx	AUTSW	NNNNN	0 *(siehe SU24)*	HR: Kundeneigene Berechtigungsprüfung
xxx	AUTSW	ORGIN	1 *(aktiviert)*	HR: Stammdaten
xxx	AUTSW	ORGPD	0 *(nicht aktiviert)*	HR: Strukturelle Berechtigungsprüfung (keine strukturelle Berechtigung aus Organisationsmanagement)
xxx	AUTSW	ORGXX	1 *(aktiviert)*	HR: Stammdaten - erweiterte Prüfung
xxx	AUTSW	PERNR	0 *(nicht aktiviert)*	HR: Stammdaten Personalnummernprüfung *(zu den vorgenannten Obj. logisches **Oder**)*
xxx	AUTSW	VACAU	*(nein)*	Berechtigungen Vakanzen pflegen/einschalten

Tab. 2: Berechtigungshauptschalter AUTSW in Tabelle T77S0 (Bsp.) [2]

Entsprechend der dargestellten Vorgaben werden die HR-Berechtigungsobjekte in den Berechtigungen der Rollendefinitionen ausgeprägt.

Die wichtigsten HR-Berechtigungsobjekte im Detail:

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne/-tabelle
P_ABAP	HR: Reporting	REPID	ABAP-Reportname	D:PROGNAME
		COARS	Vereinfachungsgrad der Berechtigungs-prüfung	D:COARS [1=Infotyp-berechtigung ist unabhängig von org. Zuordnung 2 oder *=Report soll ungeprüft ausgeführt werden]
P_BEN	Arbeitgeberleistungs-bereich	PBEN_AREA	Arbeitgeberleistungs-bereich	D:BEN_AREA T5UB3
		ACTVT	Aktivität	TACT/TACTZ

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne/-tabelle
P_CH_PK	Pensionskasse: Kontenzugriff	KONNR	Nummer PK-Konto	DT:P02K_KONNR
		AUTGR	Berechtigungsgruppe für PK-Konten (HR-CH)	D:P02K_AUTGR T5CPG/T5CPH
		PKKLV	Berechtigungslevel für Konten (HR-CH)	D:P02K_PKKLV [R/**W/X**/-]
PLOG	Personalplanung und -entwicklung	PLVAR	Planvariante	T777P/T778P
		OTYPE	Objekttyp	T778O
		INFOTYP	Infotyp	D:INFOTYP T777D, T778T, T582S
		SUBTYP	Subtyp	D:SUBTYP T591S/T778U
		ISTAT	Planungsstatus	T777S/T778S
		PPFCODE	Funktionscode	T77FC/T77FD
P_APPL	Bewerber	INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U
		AUTHC	Berechtigungslevel	D:AUTHC_D [R=Read; M=Matchcode; **W=Write; D=Change lock-indicator; E=Edit (Write) with lock; S=Symmetric check; *=all**]
		PERSA	Personalbereich	T500P
		APGRP	Bewerbergruppe	T750K
		APTYP	Bewerberkreis	T750F
		VDSK1	Organisationsschlüssel	T527/T527A/ T527O
		RESRF	verantw. Pers.referent	D:SACHA
P_ORGIN [Berechtigungs-hauptschalter ORGIN der Gruppe AUTSW in T77S0]	Stammdaten	INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U
		AUTHC	Berechtigungslevel	D:AUTHC_D [siehe P_APPL]
		PERSA	Personalbereich	T500P
		PERSG	Mitarbeitergruppe	T501
		PERSK	Mitarbeiterkreis	T503K/T503T
		VDSK1	Organisationsschlüssel	T527/T527A/ T527O

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne/-tabelle
P_ORGXX [Berechtigungs-hauptschalter ORGXX der Gruppe AUTSW in T77S0]	Stammdaten – Erweiterte Prüfung	INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U
		AUTHC	Berechtigungslevel	D:AUTHC_D [siehe P_APPL]
		SACHA	Sachbearbeiter für Abrechnung	D:SACHA T526
		SACHP	Sachbearbeiter für Personalstammdaten	D:SACHA T526
		SACHZ	Sachbearbeiter für Zeiterfassung	D:SACHA T526
		SBMOD	Sachbearbeitergruppe	
P_PCLX	Cluster	RELID	Bereichskennung für Cluster	D:RELID_PCL T52RELID
		AUTHC	Berechtigungslevel	D:AUTHC_D [R=Read; U=Update; S=Export in PCLx-Buffer without DB-Change]
P_PCR	Personalverwal-tungssatz	ABRKS	Abrechnungskreis	T549A
		ACTVT	Aktivität	TACT/TACTZ
P_PE01	Personalrechen-schemata	P_AUTHPE01	HR-Schema: Berechtigung	D:P_AUTHPE01 [S=Show; **U=Update**] T52C0/T52C1
P_PE02	Personalrechen-regel	P_AUTHPE02	Personalrechenregel: Berechtigung	D:P_AUTHPE02 [S=Show; **U=Update**] T52C5
P_PERNR [Berechtigungs-hauptschalter PERNR der Gruppe AUTSW in T77S0]	Stammdaten Personalnummern-prüfung	AUTHC	Berechtigungslevel	D:AUTHC_D [siehe P_APPL]
		PSIGN	Interpretation einer zugeordneten Personalnummer	[I= Die eigene PERNR hat mehr Berecht. als andere PERNR. E= Der Benutzer hat keine Berecht. für seine eigene PERNR.]
		INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne/-tabelle
P_PYEVDOC	Abrechnungsbeleg	BUKRS	Buchungskreis	T001
		AKTVT	Aktivität	TACT/TACTZ
P_PYEVRUN	Buchungslauf	P_EVTYP	Lauftyp	D:P_EVTYP T52EV
		P_EVSIMU	Buchungslauf: Simulationskenn-zeichen	D:XFELD
		ACTVT	Aktivität	TACT/TACTZ
P_TCODE	Transaktionscode (HR)	TCD	Transaktionscode	TSTC/TSTCT
P_CERTIF	Bescheinigungs-wesen	MOLGA	Ländergruppierung	T500L/T500T
		BESNR	Bescheinigungs-nummer	T704E
		AUTHC	Berechtigungslevel	D:AUTHC_D [E=Erstellung über Option Einzelerfassung; S=Erstellung über Option Schnellerfassung; A=Anzeigen über Option Bescheinigungs-druck; D=Drucken ü. “; L=Löschen ü. “; F=Freigeben ü. “]
P_DE_BW	Bescheinigungs-wesen SAPScript	BEWID	Bescheinigungsidentif.	D:P01_BEWID T5DF0
		BSUBJ	Sachgebietskennung	DT:P01_BSUBJ T5DF5
		BACT	Aktivitäten für Bescheinigungswesen	D:P01_BACT
P_ORGINCON [Kontext-Berechtigungs-hauptschalter INCON der Gruppe AUTSW in T77S0]	Stammdaten mit Kontext (ab 4.7)	INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U
		AUTHC	Berechtigungslevel	D:AUTHC_D [siehe P_APPL]
		PERSA	Personalbereich	T500P
		PERSG	Mitarbeitergruppe	T501
		PERSK	Mitarbeiterkreis	T503K/T503T
		VDSK1	Organisationsschlüssel	T527/T527A/ T527O
		PROFL	Berechtigungsprofil	D:PROFL T77PQ

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne/-tabelle
P_ORGXXCON [Kontext-Berechtigungs-hauptschalter XXCON der Gruppe AUTSW in T77S0]	Stammdaten – Erweiterte Prüfung mit Kontext (ab 4.7)	INFTY	Infotyp	D:INFOTYP T777D, T582A
		SUBTY	Subtyp	D:SUBTY [T591S,] T778U
		AUTHC	Berechtigungslevel	D:AUTHC_D [siehe P_APPL]
		SACHA	Sachbearbeiter für Abrechnung	D:SACHA T526
		SACHP	Sachbearbeiter für Personalstammdaten	D:SACHA T526
		SACHZ	Sachbearbeiter für Zeiterfassung	D:SACHA T526
		SBMOD	Sachbearbeitergruppe	
		PROFL	Berechtigungsprofil	D:PROFL T77PQ
P_TRAVL	Reisedaten (Management)	BUKRS	Buchungskreis	T001
		AUTHS	HR-Reise: Status NEU beim Sichern der Reise	D:AUTHS
		AUTHF	HR-Reise: Operation und Status ALT	D:AUTHF
		AUTHP	HR-Reise: Prüfung der Personalnummer	D:AUTHP
		KOSTL	Kostenstelle	CSKS
		PERSG	Mitarbeitergruppe	T501
		PERSK	Mitarbeiterkreis	T503K/T503T
		VDSK1	Organisationsschlüssel	T527/T527A/ T527O
		WERKS	Personalbereich	[T500P]
		PTZUO	Mitarbeitergruppierung Reisemanagement	D:PTZUO T702Y
P_PEPSVAR	Personaleinsatz-planung: Benutzerabhängige Sortiervarianten	P_PEPSVAR	Variante	DT:PEPSVAR_AUTH
S_MWB_FCOD	BC-BMT-OM: Erlaubte Funktions-codes für Managers' Desktop	MWBFCODE	Funktionscode	T77MWBFCD

* D: Domäne; DT: Datentyp

Tab. 3: Ausgesuchte Berechtigungsobjekte

Der in Tab. 2 erwähnte Berechtigungshauptschalter, der das Zuschalten zusätzlicher Prüfroutinen innerhalb des Customizing ermöglicht (aktivierungsfähiger Standard), passt die Ausprägungen der Berechtigungen automatisch an die Einstellungen der Hauptschalter-objekte an (s. Tabelle USOBT).

Drei der relevanten Werte zur Zugriffssteuerung bestimmter Funktionen sind die Prüfungs- und Status-Schalter des Reisemanagements. Die hier möglichen Werte für AUTHS/AUTHF/ AUTHP sind:

Berechtigungsfeld	Position 1	Position 2	Position 3
AUTHS	1=Antrag	0=offen	
AUTHS	2=Antrag genehmigt	1=abzurechnen	
AUTHS	3=Reise	3=storniert	
AUTHS	4=Reise genehmigt	*=alle Status	
AUTHS	5=Antrag wartet		
AUTHS	6=Reise wartet		
AUTHS	*=alle Status		
AUTHF	R=Lesen der Reisedaten	Leer=Neue Reise	Leer=Neue Reise
AUTHF	W=Anlegen, Ändern, Kopieren von Reisedaten	1=Antrag	0=offen
AUTHF	D=Löschen von Reisedaten	2=Antrag genehmigt	1=abzurechnen
AUTHF	X=Abrechnen der Reisedaten	3=Reise	2=abgerechnet
AUTHF		4=Reise genehmigt	3=storniert
AUTHF		5=Antrag wartet	4=gebucht
AUTHF		6=Reise wartet	*=alle Status
AUTHF		*=alle Status	
AUTHP	O=nur die eigene PERNR		
AUTHP	E=alle PERNR, nur nicht die eigene PERNR		
AUTHP	*=alle PERNR		

Tab. 4: Ausprägungen im Reisemanagement

[Im Feld AUTHS ist die Ausprägung des Status' beim Sichern der Reisedaten zu definieren. Das Feld ist zweistellig. Die erste Position definiert den Antrags- und die zweite den Abrechnungsstatus der angeforderten Reise. Im Feld AUTHF ist die Ausprägung der Operation und des Status' der angeforderten Reise zu definieren. Das Feld ist dreistellig. Die erste Position definiert die gewünschte Operation, die zweite den Antrags- und die dritte den Abrechnungsstatus der angeforderten Reise. Im Feld AUTHP ist die Ausprägung der Prüfung der Personalnummer zu definieren.]

Wie zu sehen ist, kann die Berechtigungssteuerung in HR sehr umfangreich gestaltet werden. Neben der Steuerung, welche Daten in welcher Form bearbeitet werden dürfen, kommt auch die Strukturgebung nicht zu kurz, was grundsätzlich erheblich zu einer sinnvollen Definition von Rollen / Arbeitsplätzen beiträgt. Was ebenfalls angenehm ist, ist die Steuerung auf den eigenen Datensatz. Wenn ein Personalsachbearbeiter Änderungen an Infotypen wie beispielsweise 0008, 0014, 0015 und anderen durchführen soll, so ist steuerbar, dass er dies nicht in seinem Stammsatz ändern kann.

Neben der Berechtigungsobjektausprägung haben selbstverständlich die Transaktions-berechtigungen einen besonderen Stellenwert. Entsprechend der Sensibilität der involvierten Daten können einige Transaktionen als kritisch erachtet werden. Jedes Unternehmen muss hier selbstverständlich für eine eigene Abgrenzung sorgen.

Transaktion	Beschreibung
PA03	Personalverwaltungssatz pflegen
PA10	Personalakte
PA20	Personalstammdaten anzeigen
PA30	Personalstammdaten pflegen
PA40	Personalmaßnahmen
PA41	Ein-/Austrittsdatum ändern

Transaktion	Beschreibung
PA61	Zeitdaten pflegen
PA62	Listerfassung Zusatzdaten
PA63	Zeitdaten pflegen
PA70	Schnellerfassung
PA71	Schnellerfassung Zeitdaten
PACK	HR-CH: Pensionskasse
PACN	Nummernkreispflege für Konten
PACO	Konten-/Buchungspflege Pensionskasse
PACP	Pensionskasse, Oberfläche
PB00	Bewerberverwaltung
PB10	Ersterfassung Bewerberstammdaten
PB30	Bewerberstammdaten pflegen
PB40	Bewerbermaßnahmen
PB60	Bewerbervorgänge pflegen
PC0*	Abrechnung
PE00	Startet Transaktionen PE01,PE02,PE03
PE01	HR: Pflege von Personalrechenschemen
PE01N	Editor für Abrechnungsschemen
PE02	HR: Pflege von Personalrechenregeln
PE02N	Editor für Personalrechenregeln
PE03	HR: Merkmale
PE04	Funktionen und Operationen anlegen
PMESIM	manuelle Abrechnungssimulation
PMSI	Abrechnungssimulation
PO01	Arbeitsplatz pflegen
PO03	Stelle pflegen
PO10	Organisationseinheit pflegen
PO11	Qualifikation pflegen
PO13	Planstelle pflegen
PPCP	Laufbahnplanung
PR00	Reisekosten
PR20	Anlegen einer Reise
PRCC	Kreditkartenclearing
PRPL	Reiseplan anlegen
PT00	Zeitwirtschaft
PT01	Arbeitszeitplan hinzufügen
PT02	Arbeitszeitplan ändern
PT60	Zeitauswertung
PT61	Zeitnachweis
PU00	Personaldaten löschen
PU01	Lösche aktuelles Abrechnungsergebnis
PU03	Abrechnungsstatus ändern
PU11	Zusatzversorgung öffentlicher Dienst
PU30	Lohnartenpflege
PU90	Bewerberdaten löschen
PU95	HR: Pflege log. Views & Lohnartengruppen
PU96	HR: Lohnartengruppen pflegen
PU97	HR: Logische Viewpflege

Tab. 5: Mögliche überprüfungsrelevante Transaktionen (Bsp.)

Die Berechtigungen, die bei Aufruf der kritischen Transaktionen benötigt werden, lassen sich über die Einträge der Tabelle USOBT wie oben erwähnt herausfiltern. Customizing-abhängige Felder sind in dieser Darstellung natürlich nicht als kritisch gekennzeichnet, diese muss der Revisor selbständig erkennen. Er muss hierbei die kritischen Feldeinträge und -konstellationen identifizieren und auf diese prüfen.

TR	Transaktionstext	Objekt	Feld1 mit Wert	Feld2 mit Wert	Feld3 mit Wert	Feld4 mit Wert	Feld5 mit Wert	Feld6 mit Wert	Feld7 mit Wert
PA10	Personalakte	PLOG	INFOTYP	SUBTYP	ISTAT	OTYPE	PLVAR	PPFCODE	
			1001	*	*	C, O, P, Q, S	$PLVAR	*	
		P_ORGIN	INFTY	SUBTY	AUTHC	PERSA	PERSG	PERSK	VDSK1
					R				
		P_PCLX	RELID	AUTHC					
			PC, TX	R					
		P_PERNR	INFTY	SUBTY	AUTHC	PSIGN			
PA20	Personalstamm anzeigen	PLOG	INFOTYP	SUBTYP	ISTAT	OTYPE	PLVAR	PPFCODE	
			1001	*	*	C, O, P, Q, S	$PLVAR	*	
		P_ORGIN	INFTY	SUBTY	AUTHC	PERSA	PERSG	PERSK	VDSK1
					R				
		P_PCLX	RELID	AUTHC					
			PC, TX	R					
		P_PERNR	INFTY	SUBTY	AUTHC	PSIGN			
PA61	Zeitdaten pflegen	P_ORGIN	INFTY	SUBTY	AUTHC	PERSA	PERSG	PERSK	VDSK1
					*				
		P_PCLX	RELID	AUTHC					
			PC, TX, B1, B2	*					
		P_PERNR	INFTY	SUBTY	AUTHC	PSIGN			
PA70	Schnellerfassung	PLOG	INFOTYP	SUBTYP	ISTAT	OTYPE	PLVAR	PPFCODE	
			1001	*	*	C, O, P, Q, S	$PLVAR	*	
		P_ORGIN	INFTY	SUBTY	AUTHC	PERSA	PERSG	PERSK	VDSK1
					R				
		P_PCLX	RELID	AUTHC					
			PC, TX	*					
		P_PERNR	INFTY	SUBTY	AUTHC	PSIGN			

Tab. 6: Einträge der Tabelle USOBT zu bestimmten Transaktionen (Bsp.)

Fazit

Die Darstellungen entsprechen natürlich kaum dem tatsächlich möglichen Komplexitätsgrad des HR-Umfeldes, aber sie zeigen bereits deutlich, welche Umgebung den Revisor bei einer Prüfung erwartet.

Die Rollen / Arbeitsplätze müssen eindeutig definiert und voneinander abgegrenzt sein. Auch schließen sich üblicherweise Vermischungen von Rollen bei Mitarbeitern gerade in diesem Umfeld möglicher Interessenkollisionen aus. Eine Prüfung ist neben der Berechtigungs- auch immer eine Funktionsbereitstellungsprüfung. So sind die Rollen sowohl auf der Ebene der Berechtigungsobjekte als auch der Transaktionen zu durchleuchten. Dabei ist es nahe liegend, dass Basistransaktionen wie zum Beispiel SE16, SE17, SA38, SE38 und die dazu benötigten kritischen Berechtigungsobjektausprägungen keine Verwendung in den Fachbereichsberechtigungen finden.

Wichtig ist die Erkenntnis, dass eine Nachlässigkeit im HR bei der Berechtigungsvergabe Zugriffsverletzungen nach sich ziehen kann, die im Bereich des persönlichen Empfindens weit schwerwiegender sind als erweitere Rechte im MM oder CO. Selbst wenn das Unternehmen dies ggf. anders sieht, da es sich hier kaum um wirtschaftssensible Daten handelt wie eben in anderen Modulen, können hier bei Bekanntwerden entsprechender Datenzugriffe erhebliche Spannungen entstehen. Der Vertrauensverlust der Belegschaft gegenüber neuen Funktionen wie zum Beispiel ESS und das Misstrauen der Mitarbeiterinteressenvertretung ist dann ggf. bedeutsamer als eine schnelle und mitunter nicht akzeptierte Lösung.

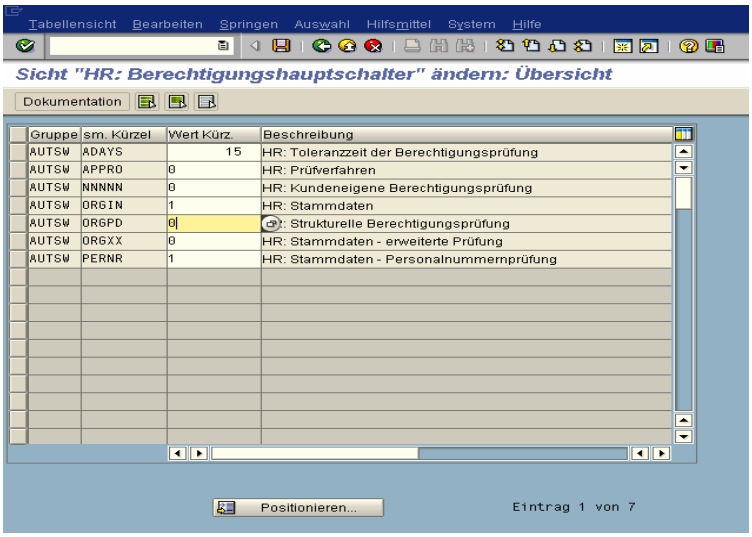
Entsprechend sollte ein Revisor auch eine sichere Hand bei der Analyse in diesem Umfeld beweisen – speziell die Administrations-, Sachbearbeitungs- (Personalmanagement und Personalabrechnung), Key-User- und Beratungsebene sind als besonders kritisch zu nennen und somit von besonderem Interesse.

Anhang

[1]: häufig gewählte Darstellung der SAP R/3 HR-Modulsicht:

Personalwirtschaft	HR-PA	Personaladministration und -abrechnung	- Personaladministration - Personalbeschaffung - Zeitmanagement - Personalabrechnung - Reisekosten
	HR-PD	Personalplanung und -entwicklung	- Organisationsmanagement - Personalentwicklung - Veranstaltungsmanagement - Personalkostenplanung - Personaleinsatzplanung - Personalinformationssystem

[2]: Berechtigungshauptschalter



ORGPD: Wert = 1 (HR: Strukturelle Berechtigungsprüfung aktivieren)

Beyer/Fischer/Jäck u.a.	SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, SAP Press/ Galileo Press, Bonn, 2003;
Brochhausen/Kielisch/Schnerring/Staeck	mySAP HR – Technische Grundlagen und Programmierung, SAP Press / Galileo Press, Bonn, 2. Auflage 2005;
Thomas Tiede	SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP), 2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, http://www.osv-hamburg.de;
Christoph Wildensee	Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht - für Basis, FI, CO, IS-U, IDEX-GE u.a.; ReVision III/2001ff, Ottokar-Schreiber-Verlag, Hamburg,http://www.osv-hamburg.de;