Revision 4.0

Christoph WIldensee

SoD-Konflikte des P2P-Prozesses in SAP

Einer der aus Unternehmenssicht kritischen Prozesse in der Abbildung in SAP ist der **Purchase-to-Pay**-Prozess (P2P), also der IT-seitig abgebildete, prozessuale Weg der Beschaffung von Waren und Dienstleistungen von der Lieferantenanlage (Stamm und CpD) über die Bestellanforderung und -auslösung bis zur Warenlieferung, Rechnungsstellung und Bezahlung dieser mit Initiierung des Zahllaufs. Dies entspricht z. B. den Transaktionen

Prozessschritt	Bsp.-Transaktionen	Prozessschritt	Bsp.-Transaktionen
Bestellanforderung	ME51*, ME52*, ME54*, ME55, ME57, ME58, ME59*	Lieferant	M-01, M-02, M-51, M-52, M-53, FK01, FK02, FK05, FK06, XK01, XK02, XK05, XK06
Bestellungen	ME21*, MEPO, ME22*, ME25, ME59*, ME3*	Wareneingang	MIGO, MIGO_GR, MB01, MB02, MB0A, MB1B
Rechnung erfassen	MIRO, MIRA, MRRL, MR01, MR02, MRBR, F-*	Zahllauf	F110, F110S, F150

Tab. 1: Beispiel-Transaktionen zu den einzelnen P2P-Schritten.

In der PRev Revisionspraxis 3 / 2009 habe ich bereits über *Funktionsübernahmen in Personalunion – Rollenkollisionen in SAP* beschrieben, welche Gefahren bei einer Kombination von zwei und mehr Arbeitsplatzrollen in einem Stammsatz entste-

hen können, wenn diese Buchungskreis-eingegrenzte "read-only"- und manipulierende Rollen beinhalten. Dort ist dann unter Umständen die Kombination erheblich höher privilegiert als die Einzelrollen selbst aussagen. Auch der Weg der Analyse wird hier beschrieben, so zu den Arbeitsplatzdefinitionen und beinhalteten Rechten z. B. über die Tabellen AGR_DEFINE, AGR_USERS, AGR_10*, AGR_125*, UST04, UST10* und UST12. Natürlich wird der Hinweis auf die Tabelle USOBT gegeben, die die notwendigen, funktionalen Berechtigungsobjektausprägungen zur Nutzung der Transaktionen beinhaltet. Hier kann also geschaut werden, welche Objektausprägungen im Stammsatz vorhanden sein müssen, damit eine Transaktion auch ausgeführt werden kann. Wichtig ist an dieser Stelle der Hinweis, dass es dazu kundenanpassbare Möglichkeiten gibt, d. h. im Standard notwendige Objektausprägungen können kundenseitig angepasst werden über die Tabellen USOBT_C (bzw. USOBX mit USOBX_C).

Was bedeutet dieser Schritt insgesamt?
In vielen Unternehmen werden Einzelrollen bereitgestellt, die auf der Ebene der Arbeitsplatzrollen kombiniert werden und somit die Gesamtrolle bilden. Die Transaktionscodes werden in den funktionalen Einzelrollen nicht inkludiert, sondern als separate Einzelrolle mit allen notwendigen, arbeitsplatzbezogenen Transaktionscodes hinzugefügt. Ein Arbeitsplatz ist also folglich eine Kombination aus einer Vielzahl von funktionalen Einzelrollen mit privilegierten Objektausprägungen im Bereich F_*, M_*, K_* usw. und einer oder wenigen Einzelrollen, die nur Ausprägungen zu S_TCODE beinhalten (funktional & transaktional; Konzept der Mehrfachverwendung von Einzelrollen in Sammel-/Arbeitsplatzrollen). Die **Gefahr** besteht darin, dass aufgrund des gezielten Eingrenzens der Transaktionscodes stärker als notwendig privilegierte Berechtigungsobjektausprägungen in den Einzelrollen vorliegen, weil man davon ausgeht, dass ein Aufrufen kritischer Transaktionen trotz Vorliegens stark ausgeprägter Berechtigungsobjekte im Stammsatz nicht funktioniert. Denn wenn nun ergänzende Add-On-Rollen dem Stammsatz hinzugefügt werden, die ggf. für eine Ausnahmesachbearbeitung einen kritischen Transaktionscode beinhalten, kann sich hier eine **hochprivilegierte Rollenkumulation** ergeben.

Der Artikel in der PRev 3/2009 beschränkt sich auf die Sicht der Berechtigungsobjekte des Moduls FI, also der F-Objekte. Um hier eine besondere Sicht auf kritische Kombinationen zu ermöglichen, muss diese Sicht erweitert werden auf M-Objekte. "**Segregation of Duties**", kurz SoD, beinhaltet den funktionalen Konflikt, Aufgaben unzulässig verantwortungsübergreifend im System lösen zu können. In jeder Organisation werden die Aufgaben Verantwortungsträgern in definierten Grenzen des IT-Systems überlassen. Die prozessualen Daten werden über die erwartete Funktionswahrnehmung angereichert und im Rahmen der Verantwortungsübernahme prozessiert.

Wenn jedoch von der Bestellung über den Wareneingang bis zum Rechnungsausgleich und Zahllauf alle Schritte in einer Person vereint sind, wird diese Gefahr als Möglichkeit des Ausnutzens zum Schaden des Unternehmens wahrgenommen. Auch Prozessteilstrecken können sehr kritisch sein. Obwohl jeder Schritt umfänglich protokolliert wird, wird diese Historie in vielen Unternehmen im Rahmen der operativen Fachbereichs-IKS-Maßnahmen kaum beachtet. Allerdings ist hier viel Bewegung, da es Systeme gibt, die kritische Datenwege und auch Verantwortungsabgrenzungen zum funktionalen Prozessweg prüfen können (data & process mining), so z. B. Celonis. Dieser Artikel soll in Kürze darlegen, dass trotz des Mengengerüstes das implementierte Berechtigungskonzept zur Verhinderung von SoD-Konflikten effizient analysiert werden kann.

Prozessuale Analyse von Konfliktauslösern
Die Tabelle USOBT zeigt für die Prozessschritte des P2P-Prozesses (Transaktionen M* und F*) mehr als 40.000 Einträge. Dies verdeutlicht zwar, dass es wohl viele Ansätze zur Prüfung gibt, die undifferenzierte Sicht auf diese Zahl zeigt jedoch nicht, dass es zunächst einfach zu handhabende Ansätze zur Prüfung gibt, die sich bereits aus dem Rollenmodell selbst ergeben.

Triggerrollen
Was wir grundsätzlich wissen, ist, dass im Bereich des Einkaufs für **Bestellungen** sechs Berechtigungsobjekte und für Rahmenbestellungen ebenfalls sechs Objekte wesentlich sind. Dies sind für die Bestellungen die Objekte M_BEST_BSA (Belegart in Bestellungen), M_BEST_EKG (Einkaufsgruppe), M_BEST_EKO (Einkaufsorganisation), M_BEST_LGO (Werk, Lagerort), M_BEST_WRK (Werk) und M_BEST_EXP (Progress-Tracking-Gruppe), für die Kontrakte/Rahmenverträge die Objekte M_RAHM_BSA, M_RAHM_EKG, M_RAHM_EKO, M_RAHM_LGO, M_RAHM_WRK und M_RAHM_STA (Status).

Sofern für die Fachbereiche eine Plattform für alltägliche Materialien bereitgestellt wird (Katalogbestellungen) oder Fachbereiche z. B. Abrufe auf Rahmenverträge durchführen können, kann es sein, dass fünf der sechs M_BEST-Objekte in hoher Ausprägung in einer Viel-

zahl von Fachbereichseinzelrollen vorliegen und nur ein Objekt die Steuerung für die funktionale Eingrenzung tatsächlich vornimmt. Ggf. gibt es noch bei den Objekten zum Lagerort und Werk eine Eingrenzung in Fachbereichseinzelrollen. Ist dies insgesamt der Fall, sind diese Fachbereichsrollen also nicht das Problem, sondern die **Triggerrolle** mit einem **Vollzugriff** (ACTVT – Aktivität = 01 oder "*") auf (nahezu) alle Belegarten (M_BEST_BSA, Ref. T161). Lässt sich ggf. sogar eine bestimmte Belegart als besonders kritisch oder nur durch den Einkauf auslösend identifizieren, können die Triggerrollen herausgelöst werden, die neuralgisch im Prozess wirken. Diese können wiederum über die SAP-Tabelle AGR_AGRS als Child zur Identifikation der Arbeitsplatzrollen genutzt werden, die diese exponierten Einzelrollen beinhalten. Wurden diese wiederum erkannt, können über die Tabelle AGR_USERS die Stammsätze dargelegt werden, denen die Arbeitsplätze zugewiesen wurden. In Kombination mit beispielsweise der Tabelle USER_ADDR können die organisatorischen Daten zum User bereitgestellt werden, um die beschäftigtenbezogenen Stammdaten herauszufiltern, deren prozessuale Funktionswahrnehmung nicht eindeutig ist. M_RAHM-Objekte mit ACTVT = 01 oder "*" gehören ebenfalls nur in den Einkauf.

Im Bereich der **Zahlungsabwicklung** können ebenfalls die Triggerrollen ermittelt werden. Es handelt sich um Objekte der Art F_BKPF*. Auch hier gilt, dass diese Objekte in ca. 250 F- und M-Transaktionen in höherer Ausprägung genutzt werden. Sucht man insbesondere die Objektausprägung F_BKPF_BUK mit Aktivität 01 und die Generalausprägung "*" (für den Überblick auch 02, 06 [ändern, löschen]), lassen sich die Einzelrollen und über den zuvor genutzten Weg der Tabellen AGR_AGRS und AGR_USERS die Arbeitsplatzrollen feststellen, die eine **exponierte Stellung im Berechtigungskonzept** einnehmen. Gleiches gilt als dritter Sichtaspekt für die Objekte F_REGU_KOA und F_REGU_BUK (Automatische Zahlung: Kontoarten und Buchungskreis), die für die **Zahllaufsteuerung** mit der Ausprägung 21 (und somit auch mit "*") verantwortlich sind.

Zuletzt soll die Anlage und Nutzung von **Lieferanten** erwähnt werden. Zur Nutzung im Prozess ist die Bedienung eines Lieferantenstammsatzes und die CpD-Nutzung als zentrales Objekt zu erwähnen.

Sofern diese Prozesseinzelschritte (oder auch teilkritische Stränge) in einer Hand liegen, ist eine Anpassung dringend geboten, da es sich mit an Sicherheit grenzender Wahrscheinlichkeit um einen **SoD-Konflikt** handelt.

Warum steht hier aber nichts von Transaktionsberechtigungen?
Zunächst ist davon auszugehen, dass die am Prozess wesentlich beteiligten Rollen in der Sachbearbeitung des Einkaufs und des Finanz- und Rechnungswesens/Kreditorenbuchhaltung usw. die notwendigen Transaktionen aufweisen. Zusätzlich muss neben den Transaktionsberechtigungen auch geprüft werden, ob eine Substitution vorliegt. Haben die Berechtigten z. B. die Transaktion **SA38, OODR, START_REPORT** oder ähnliche Aufrufvarianten, bedeutet dies, dass sie die zugrunde liegenden Programme (Typ = 1 beachten, siehe Tabellen TRDIR [SUBC] und TSTC), sofern sie Kenntnis von deren Namen haben, aufrufen können. Im Bereich der M-Transaktionen kann man hierüber viele fehlende Transaktionscodes substituieren, F-Transaktionen allerdings wenige. Da die Objektsteuerungsfelder im Stammsatz jedoch in hoher Ausprägung vorliegen, erhalten sie in solchen Fällen keine Ablehnung. Insofern ist es oft zu kurz gegriffen, ausdrücklich auf Transaktionsberechtigungen zur Aufgabenbegrenzung abzuzielen. Es ist sinnvoll, wesentliche der kritischen Transaktionscodes in die Abfrage zu integrieren, jedoch offeriert SAP eine Vielzahl an Möglichkeiten, Funktionen aufzurufen. Ob man alle durch Abfragen erwischen kann, ist fraglich. Es ist wesentlich, die **neuralgischen Einzelrollen** und die **Arbeitsplatzrollen** herauszufiltern, die durch diese Einzelrollen mit hohen Rechten gespeist werden, um diese dann **funktional einzuhegen**.

Anpassungsbedarf
Die Sicht auf die auslösenden Einzelrollen in den Arbeitsplätzen bedeutet, dass darauf zu achten ist, dass eine Anpassung einer Einzelrolle möglicherweise mehrere Arbeitsplätze betrifft und deren Sachbearbeitungsfunktion beeinträchtigt. Sofern nur wenige Arbeitsplätze betroffen sind, kann die dort ggf. notwendige Ausprägung, die entzogen werden soll, durch eine andere Einzelrolle des Arbeitsplatzes substituiert werden, was bedeuten kann, dass ein Entzug in der Einzelrolle möglich ist. Wird das zu entziehende Recht jedoch nicht durch eine andere Einzelrolle bei demjenigen, der das Recht benötigt, bereitgestellt, muss ggf. eine Einzelrollenaufspaltung und separate Zuweisung erfolgen. Solche Punkte erweitern das Mengengerüst der Einzelrollen und erhöhen die Gefahr, dass zu einem späteren Zeitpunkt diese ergänzenden bzw. separierenden Kleinstrollen in anderen Rollen Einzug finden und das "Need-To-Know"-Prinzip langfristig unterlaufen.

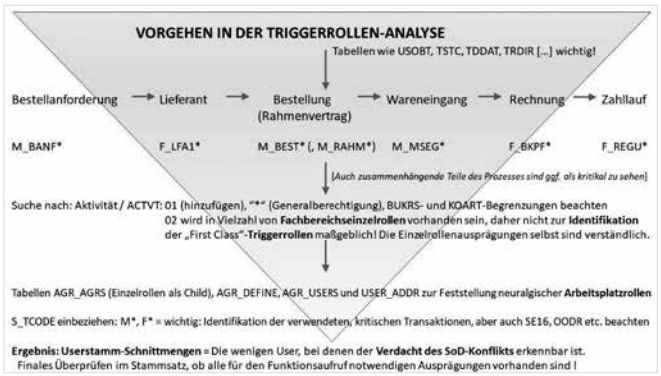

Abb. 1: Mögliches Vorgehen zur Identifikation von SoD-Konflikten.

Fazit

Wir sind im Berechtigungswesen von SAP und den begrenzenden Elementen der Rollendefinition schon aufgrund der schieren Menge an Ausprägungsmöglichkeiten in einem Zielkonflikt. Zum einen soll das Gerüst möglichst übersichtlich bleiben, um den Administrationsaufwand gering zu halten, denn die Steuerung ist kein Selbstzweck und mit hohen, internen Kosten verbunden. Gleichsam sind aber auch die SoD-Problematik und die Risiken des prozessualen Weges im Auge zu behalten und zu lösen. Es ist kompliziert, und Lösungen sind selten einfach. Jedoch ist mit dem Fokus auf die **begrenzenden**, **neuralgischen Triggerrollen** der wesentliche und effiziente Schritt zur Risikomitigierung getan. Automatisierte Verfahren zeigen diese Punkte zwar sehr gut strukturiert. Aber eine Bewertung der Analyseergebnisse, auch im Hinblick auf unternehmensinterne Vorgaben und Präferenzen, und eine Ableitung möglicher Anpassungsvarianten und die Wirkungsanalyse dieser bleibt jedoch der Revision und der SAP-Administrationsebene in der Detailsicht vorbehalten.

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

Literatur

Harmes (2018): https://rz10.de/sap-berechtigungen/sap-grc/sod-troubleshooting-funktionstrennungskonflikte-in-sap/.

Harmes (2019): https://rz10.de/sap-berechtigungen/verhalten-von-berechtigungen-nach-sap-upgrades/.

Lehnert et al. (2016): SAP-Berechtigungswesen – Konzeption und Realisierung, 3. Auflage, SAP Press, Rheinwerk Publishing.

Wildensee (2009): Funktionsübernahmen in Personalunion – Rollenkollisionen in SAP, in: PRev Revisionspraxis 3 / 2009, S. 153-162.

Wildensee (2015): Analyse der Einkaufsbestellberechtigungen in SAP ERP In: ZIR 3/2015, S. 112-120.

Anlage

Beispiel: Ausgesuchte Schritte im Prozess mit Objektausprägungen		
Bestellungen anlegen		
M_BEST_BSA	Aktivität	01 (Anlegen), 09 (Preisanzeige) oder "*"
	Einkaufsbelegart	"*" oder Einträge gem. Tabelle T161 (Einkaufsbelegarten), Einträge wählen, die ausdrücklich durch den Einkauf eingesteuert werden
M_BEST_EKG	Aktivität	01 (Anlegen), 09 (Preisanzeige) oder "*"
	Einkäufergruppe	"*" oder Einträge gem. Tabelle T024 (Einkaufsgruppen)
M_BEST_EKO	Aktivität	01 (Anlegen), 09 (Preisanzeige) oder "*"
	Einkaufs-organisation	"*" oder Einträge gem. Tabelle T024E (Einkaufsorganisationen)
M_BEST_WRK	Aktivität	01 (Anlegen) oder "*"
	Werk	"*" oder Einträge gem. Tabelle T001W / T024W (Werke / zulässige Einkaufsorganisationen zum Werk)
Wareneingang buchen		
M_MSEG_BWE	Aktivität	01 (Anlegen) oder "*"
	Bewegungsart	"*" oder Einträge gem. Tabelle T156 (Bewegungsart)
M_MSEG_WWE	Aktivität	01 (Anlegen) oder "*"
	Werk	"*" oder Einträge gem. Tabelle T001W
Eingangsrechnungsbeleg buchen		
F_BKPF_BUK	Aktivität	01 (Anlegen), 10 (Buchen), 43 (Freigeben) oder "*"
	Buchungskreis	"*" oder ausgesucht-wichtige Einträge gem. Tabelle T001
F_BKPF_BES	Aktivität	01 (Anlegen), 77 (Vorerfassen) oder "*"
	Berechtigungs-gruppe	"*" oder Einträge gem. Tabelle TBRG
F_BKPF_BEK	Aktivität	01 (Anlegen), 77 (Vorerfassen) oder "*"
	Berechtigungs-gruppe	"*" oder Einträge gem. Tabelle TBRG
F_BKPF_BLA	Aktivität	01 (Anlegen), 10 (Buchen), 43 (Freigeben) oder "*"
	Berechtigungs-gruppe	"*" oder Einträge gem. Tabelle TBRG
F_BKPF_GSB	Aktivität	01 (Anlegen), 77 (Vorerfassen) oder "*"
	Geschäftsbereich	"*" oder Einträge gem. Tabelle TGSB
F_BKPF_KOA	Aktivität	01 (Anlegen), 43 (Freigeben), 77 (Vorerfassen) oder "*"
	Kontoart	"*" oder Einträge gem. Domäne KOART

F_FAGL_SEG	Aktivität	01 (Anlegen), 77 (Vorerfassen) oder "*"
	SEGMENT	"*" oder Einträge gem. Tabelle FAGL_SEGM
	GLRRCTY	"*" oder Einträge gem. Domäne RRCTY
Zahllauf durchführen		
F_REGU_BUK	Buchungskreis	"*" oder ausgesucht-wichtige Einträge gem. Tabelle T001
	Aktion für autom. Abläufe	"*" oder 02, 03 (Parameter bearbeiten und anzeigen), 11, 12, 13, 14, 15, 16 (Vorschlag ausführen, bearbeiten, anzeigen, löschen, Vorschlag Zahlungsträger erstellen, LS-Ankündigung erstellen), 21, 23 (ZL ausführen, anzeigen), 24 (ZL Zahlungsdaten löschen), 25, 26 (ZL Zahlungsträger erstellen, löschen), 31 (Zahlungsträger drucken manuell)
F_REGU_KOA	Kontoart	"*" oder gem. Domäne KOART
	Aktion für autom. Abläufe	"*" oder 02, 03, 11, 12, 13, 14, 15, 16, 21, 23, 25, 26, 31

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.