SAP SoD-Konflikte analysieren

Finden der maßgeblichen Trigger-Rollen

Christoph Wildensee, 2023

Segregation of Duties

- Kurz SoD, beinhaltet den funktionalen Konflikt, Aufgaben **unzulässig verantwortungsübergreifend** im System lösen zu können.

- In jeder Organisation werden die Aufgaben Fachbereichen / 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. Dabei können auch Prozessteilstrecken kritisch sein.

- Obwohl jeder Schritt umfänglich **protokolliert** wird, wird diese **Historie** in vielen Unternehmen im Rahmen der operativen Fachbereichs-**IKS**-Maßnahmen **kaum beachtet**.

  Wer schaut schon nach, wer Lieferantenstammdaten wie die Bankverbindung ändert? Oder Bestellungen auslöst? Wer bucht den Wareneingang? Wer bucht die Eingangsrechnung und wer startet den Zahllauf?

- **Wir gehen davon aus, dass alles seine Richtigkeit hat. Wer aber nicht regelmäßig umfänglich analysiert, sollte die Fehlerquellen über das Role Model verhindern.**

Wie können wir einfach und effizient solche Punkte prüfen?

- Man könnte Werbung für CheckAud & Co. machen und es einsetzen, doch die Wahrheit ist, Tools können Daten zuverlässig zusammenstellen, die **Interpretation der Ergebnisse bleibt aber den Prüfern überlassen**.

- Tools stellen viel zu streng Hinweise zusammen, die erst nach internen und ggf. auch externen Vorgaben qualifiziert werden müssen. => „Information Overflow“ für Prüfer/-innen

- Also müssen alle Ergebnisse manuell überprüft werden. Uneingeschränkter Vorteil bei Tooleinsatz ist allerdings, dass alle Ebenen korrekt abgearbeitet werden, Berechtigungsobjekte, Transaktionscodes, Eigenentwicklungen und Substitutionen (SA38, OODR usw.).

Vorgehen

Also KEINE Werbung

- In vielen Unternehmen werden Einzelrollen bereitgestellt, die auf der Ebene der Arbeitsplatzrollen kombiniert werden und somit die Gesamtrolle (Arbeitsplatz) bilden.

- HÄUFIG: Die Transaktionscodes werden in den funktionalen Einzelrollen nicht inkludiert, sondern als separate Einzelrolle hinzugefügt. Aber: **Arbeitsplätze weisen notwendige TA auf!**

- Ein Arbeitsplatz ist also eine Kombination aus einer Vielzahl von funktionalen Einzelrollen mit privilegierten Ausprägungen 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).

Wesentliche Punkte als Grundvoraussetzung

- Administration ist teuer !!!

- Vereinfachungen im Rollenbau sind wichtig und eröffnen gleichzeitig Vorteile für die Prüfungsebene

- Es wird lieber breit inkludiert als detail-ausgeprägt

- Was heißt das? Stärker ausprägen, um auch bei Erweiterungen die Einzelrollen nicht anpassen zu müssen.

Beispiel: Einzelrolle u.a. mit F_BKPF_BUK: ACTVT = “*“ und BUKRS = “*“ anstatt ACTVT = 01, 02, 03…. und BUKRS = <explizit aus Tabelle T001>

Werden nun z.B. durch Gesellschaftsgründung die Buchungskreise in Tabelle T001 erweitert, müssen die Einzelrollen durch die Generalausprägung nicht angepasst werden – somit Aufwand in der Rollenadministration gespart.

Prüfung im Detail (1/3)

(oder spezielle BSART aussuchen)

- Suchen der neuralgischen Trigger-Rollen => TA SUIM

=> Bestellungen: M_BEST_BSA mit BSART = “*“ und ACTVT = 01 oder “*“
Sehr wahrscheinlich, dass in der Arbeitsplatzrolle „Sachbearbeitung Einkäufer“ dies gefunden wird als Ausprägung in einer oder mehreren Einzelrollen => Verwendung in anderen Arbeitsplätzen?

=> Habe ich eine oder mehrere Einzelrollen identifiziert = Transaktion SE16 mit Tab. AGR_AGRS, Einzelrolle als Child, weitere Rollen erkannt!

=> Liste aller User-Stammsätze (Dialog, Personen), die diese Arbeitsplatzrollen aufweisen, Check, ob organisatorisch ok (Tabellen AGR_USERS mit Tab. USER_ADDR, damit Identifikation, wo User arbeiten/zugehören)

=> Selbes Vorgehen bei
- F_BKPF_BUK Belege buchen im Haupt-Buchungskreis
- F_REGU_BUK Zahllauf ausführen 21 für Haupt-BUKRS
- […]

Wahrscheinlichkeit, dass in den gefundenen Einzelrollen weitere hoch **privilegierte und notwendige Objekte** zum Aufruf der Funktionen vorhanden sind, ist **hoch**.

Prüfung im Detail (2/3)

- Check: Wer ist wer?

- Was gibt es für Regelungen im Haus bzgl. des SAP-Einsatzes und der Rollenausprägung und -nutzung?

- Darf die Administrationsebene / Moduladministration Zugriff haben? Dann fallen alle mit dieser Rolle heraus, sie dürfen! (Anzahl grundsätzlich ok? Oder zu viele? Aufgabenklärung)

- Gibt es Harmonisierungen bzgl. Prod./Test-Integr./Entw.?

- Gibt es KeyUser (besonderes Wissen, Projektmitarbeit), die ein bestimmtes Mehr an Rechten haben sollen? Auch in Prod.?

- Gibt es Rollen, die in einer wesentlichen Objektausprägung doch eingegrenzt sind, z.B. im Buchungskreis?

Prüfung im Detail (3/3) Check: Administration / Modul-Betreuung

- MODADM haben Vollzugriff ohne Gesetzeskonflikt Basis (S_DEVELOP / Entwicklerschlüssel, S_SCD0), Zugriffe aber definiert häufig ansonsten wie im Entw. und Test/Integration

- Notwendig ist eigentlich eine Trennung von **MODADM** bzgl. FI und MM, also **MODADM_FI ohne** *M_BEST_BSA mit ACTVT = 01 oder * und BSART= <expl. Eingrenz. nur für den Einkauf> oder* * und **MODADM_MM ohne** *F_BKPF_BUK mit ACTVT = 01 oder * und BUKRS =<expl. Eingrenz.> oder * und F_REGU_BUK mit FBTCH = 21 oder * und BUKRS =<expl. Eingrenz> oder ** (+ analoge) => Auswertungen

- Doch wird in den Unternehmen entschieden, diese Trennung nicht zu machen, damit sind auch die Modulbetreuer mit SoD-Konflikt implementiert => Wunsch des Unternehmens

Hilfreich => Reports: Wer hat Bestellungen, Kontrakte und Rechnungen angelegt/gebucht? (GROUP BY, COUNT(*))

Bilder beim Vorgehen

Anforderungen über die Analysetabelle USOBT identifizieren (zzgl. S_TCODE = x):

Zahllauf

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

NAME	TYPE	OBJECT	FIELD	LOW	HI
F110	TR	F_REGU_BUK	BUKRS	$BUKRS	
F110	TR	F_REGU_BUK	FBTCH	02	
F110	TR	F_REGU_BUK	FBTCH	03	
F110	TR	F_REGU_BUK	FBTCH	11	
F110	TR	F_REGU_BUK	FBTCH	12	
F110	TR	F_REGU_BUK	FBTCH	13	
F110	TR	F_REGU_BUK	FBTCH	14	
F110	TR	F_REGU_BUK	FBTCH	15	
F110	TR	F_REGU_BUK	FBTCH	21	
F110	TR	F_REGU_BUK	FBTCH	23	
F110	TR	F_REGU_BUK	FBTCH	25	
F110	TR	F_REGU_BUK	FBTCH	31	
F110	TR	F_REGU_KOA	FBTCH	02	
F110	TR	F_REGU_KOA	FBTCH	03	
F110	TR	F_REGU_KOA	FBTCH	11	
F110	TR	F_REGU_KOA	FBTCH	12	
F110	TR	F_REGU_KOA	FBTCH	13	
F110	TR	F_REGU_KOA	FBTCH	14	
F110	TR	F_REGU_KOA	FBTCH	15	
F110	TR	F_REGU_KOA	FBTCH	21	
F110	TR	F_REGU_KOA	FBTCH	23	
F110	TR	F_REGU_KOA	FBTCH	25	
F110	TR	F_REGU_KOA	FBTCH	31	
F110	TR	F_REGU_KOA	KOART	$KOART	

Bestellung anlegen

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

NAME	TYPE	OBJECT	FIELD	LOW	HIGH
ME21N	TR	M_BEST_BSA	ACTVT	01	
ME21N	TR	M_BEST_BSA	ACTVT	02	
ME21N	TR	M_BEST_BSA	ACTVT	03	
ME21N	TR	M_BEST_BSA	ACTVT	08	
ME21N	TR	M_BEST_BSA	ACTVT	09	
ME21N	TR	M_BEST_BSA	BSART		
ME21N	TR	M_BEST_EKG	ACTVT	01	
ME21N	TR	M_BEST_EKG	ACTVT	02	
ME21N	TR	M_BEST_EKG	ACTVT	03	
ME21N	TR	M_BEST_EKG	ACTVT	08	
ME21N	TR	M_BEST_EKG	ACTVT	09	
ME21N	TR	M_BEST_EKG	EKGRP	$EKGRP	
ME21N	TR	M_BEST_EKO	ACTVT	01	
ME21N	TR	M_BEST_EKO	ACTVT	02	
ME21N	TR	M_BEST_EKO	ACTVT	03	
ME21N	TR	M_BEST_EKO	ACTVT	08	
ME21N	TR	M_BEST_EKO	ACTVT	09	
ME21N	TR	M_BEST_EKO	EKORG	$EKORG	
ME21N	TR	M_BEST_WRK	ACTVT	01	
ME21N	TR	M_BEST_WRK	ACTVT	02	
ME21N	TR	M_BEST_WRK	ACTVT	03	
ME21N	TR	M_BEST_WRK	ACTVT	08	
ME21N	TR	M_BEST_WRK	ACTVT	09	
ME21N	TR	M_BEST_WRK	WERKS	$WERKS	

Rechnung zahlen

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

NAME	TYPE	OBJECT	FIELD	LOW	HIG
F-31	TR	F_BKPF_BUK	ACTVT	01	
F-31	TR	F_BKPF_BUK	BUKRS	$BUKRS	
F-31	TR	F_BKPF_GSB	ACTVT		
F-31	TR	F_BKPF_GSB	GSBER	$GSBER	
F-31	TR	F_BKPF_KOA	ACTVT	01	
F-31	TR	F_BKPF_KOA	KOART	$KOART	

Bilder beim Vorgehen

Bestellungen:

Rollen nach komplexen Selektionskriterien (15 ausgewählte Rollen)

System (Mandant) [redacted] **Geprüft von** [redacted] **Geprüft am** 21.08.2023 08:35:03

Kriterien für Standardselektion	
- Einzelrollen	X
- Sammelrollen	X
Kriterien für Benutzerzuordnung	
- Rollen unabhängig von Benutzerzuordnung	X
Kriterien für Berechtigungen	
- Berechtigungsobjekt 1	M_BEST_BSA
|- Feld ACTVT	Wert ('01' OR '*')
|- Feld BSART	Wert ('NB' OR 'GB')

Rolle	Typ	Kurzbeschreibung der Rolle
.IT:MODADM_ENTW		IT SAP Modul Administration Entw./Integr.
.IT:MODADM_PROD		IT SAP Modul Administration Produktion
.IT:NOTFALL		IT SAP Notfall
.MM:EINKAUF_ADDON_[redacted]		MM Einkauf AddOn Bestellart GB [redacted]
.MM:EINKAUF_LEITUNG_[redacted]		MM Einkauf Abteilungsleitung [redacted]
.MM:EINKAUF_SB_[redacted]		MM Einkauf Sachbearbeitung [redacted]
.MM:SAP_P[redacted]		MM Einkauf SAP A[redacted]
C:DV[redacted]_A		PP MM-DV-Koo[redacted] alle Org.ebenen
M:BANF[redacted]		MM Banf Folgefunktionen Einkaufsorg. alle
M:BANF[redacted]		MM Banf Folgefunktionen Einkaufs[redacted]
M:BE0[redacted]		MM Bestellung anlegen Eink[redacted]
M:BEG[redacted]		MM Bestellung anlegen Beste[redacted]
M:DV[redacted]		MM DV-Koor[redacted]rg.ebenen
M:E[redacted]		Allumfassende Berechtigungen
M:E_NOT		Allumfassende Berechtigungen für den Notfall-User

Nomenklatur beachten!

Modul+:+Teil-Fkt+BUKRS-Umf.+Manipulationsgrad
(_A=Add, _M=Modify, _D=Display)

z.B. NB = Normalbestellung, GB = Geheimbestellung
Welche nur durch Einkauf?

<= Arbeitsplatzrollen

<= Einzelrollen

=> Check in Tab. AGR_AGRS
(Einzelrollen als Child)

Bilder beim Vorgehen

Rechnungen:

Arbeitsplatzrollen

Buchen von RE kann man hier durchaus an einigen Stellen hinter-fragen. Sind die übrigen, notwendigen Objekte und TA vorhanden?

Einzelrollen (Auszug)

Rollen nach komplexen Selektionskriterien (48 ausgewählte Rollen)

System (Mandant) F [redacted]) **Geprüft von** [redacted] **Geprüft am** 21.08.2023 08:41:01

Kriterien für Standardselektion	
- Einzelrollen	X
- Sammelrollen	X
Kriterien für Benutzerzuordnung	
- Rollen unabhängig von Benutzerzuordnung	X
Kriterien für Berechtigungen	
- Berechtigungsobjekt 1	F_BKPF_BUK
|- Feld BUKRS	Wert ('[redacted] .00' OR "*")
|- Feld ACTVT	Wert ('01' OR "*")

Rolle	Typ	Kurzbeschreibung der Rolle
.CO:ZENTR_CONTROLLING		UE Zentrales Center Controlling [redacted]
.FI:CONTROLLING		FI Controlling
.FI:DEBITOREN_SB		FI Kontokorrent Debitoren
.FI:FAKTURIER_AUFTRAG_ANLAGEN		FI Fakturierung von Aufträgen und Pflege von Anlagen
.FI:HAUPTBUCH_SB		FI Hauptbuch/Anlagen/Abschlüsse
.FI:KREDITOREN_SB		FI Kontokorrent Kreditoren
.FI:LIQUIDITAET		FI Liquidität
.FI:PREISFINDUNG		FI Preisfindung
.FI:[redacted]		FI/CO [redacted]
.FI:STEUER		FI Steuer
.FI:TREASURY		FI Treasurymanagement
.ID:ADD_ON_FI		ID ADD ON [redacted]
.IT:ADDON_FI_DATEN_UEBERNAHME		IT AddOn FI-Datenübernahme aus Digitaler Plattform
.IT:MODADM_ENTW		IT SAP Modul Administration Entw./Integr.
.IT:NOTFALL		IT SAP Notfall
.VT:HAUPTBUCH_SB		Vertrieb Hauptbuch/Anlagen/Abschlüsse [redacted]
.VT:PM_ADDON_FINANZEN_SB		Vertrieb Produktmanagement & Marketing AddOn Finanzen Sachbearbeitung
.XX:ADDON_TABPFL_[redacted]		Add-On FI Tabellenpflege und Pflegeberechtigung für Schnittstelle zu [redacted]
.XX:TABPFL_FI		Add-On Tabellenpflege FI und Pflegeberechtigung FI
F:[redacted]		Allumfassende Berechtigungen
F:[redacted]		Allumfassende Berechtigungen ohne Berechtigung für Buchungsperiode
F:B[redacted]		Allumfassende Berechtigungen KOKRS + BUKRS alle
F:B[redacted]		Allumfassende Berechtigungen B[redacted]
F:B[redacted]		Debitoren buchen
F:B[redacted]		Hauptbuch buchen [redacted]
F:B[redacted]		Kreditoren buchen B[redacted]
F:B[redacted]		Debitoren buchen ohne B[redacted]
F:B[redacted]		Kreditoren buchen ohne B[redacted]
F:C[redacted]		Modulolle zur Menürolle [redacted]
F:D[redacted]		Debitoren buchen

Bilder beim Vorgehen

Zahllauf:

Rollen eingegrenzt

nachvollziehbar, aber:
Sind die übrigen, notwendigen Objekte und TA vorhanden?
In Teilen ja. Siehe NEXT

aber hier noch keine Sicht auf Personen

Rollen nach komplexen Selektionskriterien (24 ausgewählte Rollen)

System (Mandant) . ( ) **Geprüft von** **Geprüft am** 21.08.2023 08:44:49

Kriterien für Standardselektion	
- Einzelrollen	X
- Sammelrollen	X
Kriterien für Benutzerzuordnung	
- Rollen unabhängig von Benutzerzuordnung	X
Kriterien für Berechtigungen	
- Berechtigungsobjekt 1	F_REGU_BUK
|- Feld BUKRS	Wert ('0_)0' OR "*")
|- Feld FBTCH	Wert ('21' OR "*")

Rolle	Typ	Kurzbeschreibung der Rolle
.CO:ZENTR_CONTROLLING		UE Zentrales Center Controlling
.FI:CONTROLLING		FI Controlling
.FI:DEBITOREN_SB		FI Kontokorrent Debitoren
.FI:HAUPTBUCH_SB		FI Hauptbuch/Anlagen/Abschlüsse
.FI:KREDITOREN_SB		FI Kontokorrent Kreditoren
.FI:LIQUIDITAET		FI Liquidität
.FI:SAF		FI/CO S
.IT:ADDON_FI_DATEN_UEBERNAHME		IT AddOn FI-Datenübernahme aus Digitaler Plattform
.IT:MODADM_ENTW		IT SAP Modul Administration Entw./Integr.
.IT:NOTFALL		IT SAP Notfall
.VT:HAUPTBUCH_SB		Vertrieb Hauptbuch/Anlagen/Abschlüsse
.XX:ADDON_TABPFL_		Add-On FI Tabellenpflege und Pflegeberechtigung für Schnittstelle zu
.XX:TABPFL_FI		Add-On Tabellenpflege FI und Pflegeberechtigung FI
F		Allumfassende Berechtigungen
F:		Allumfassende Berechtigungen ohne Berechtigung für Buchungsperiode
F:B		Allumfassende Berechtigungen KOKRS + BUKRS alle
F:B		Allumfassende Berechtigungen B
F:E		Debitoren buchen
F:E		Kreditoren buchen B
F:B		Debitoren buchen ohne B
F:B		Kreditoren buchen ohne B
F:		Debitoren buchen
F:		Kreditoren buchen
F:		Allumfassende Berechtigungen für den Notfall-User

Bilder beim Vorgehen => zuerst OHNE, dann MIT TCODEs checken

- M_BEST_BSA mit NB oder * und 01 oder * Bestellungen
- F_BKPF_BUK mit NNNN oder * und 01 oder * Rechn.buchung
- F_REGU_BUK mit NNNN oder * und 21 oder * Zahllauf

Benutzer	Vollst.Name	Ben. Gruppe	Gesperrt	Gültig von	Gültig bis	Abteilung
		NOTFALL		18.12.2017	31.12.9999	
		ADMIN				
DDIC	DDIC	SUPER				
		ADMIN			31.12.9999	
	Ka	MITARBEITER		20.10.2008	31.12.9999	
HS11	Car	MITARBEITER		15.10.2007	31.12.9999	EK
	N	NOTFALL				
		ADMIN				
U	Christ	MITARBEITER		10.01.2022	01.11.2023	
U	As	MITARBEITER		27.09.2022	31.12.2023	
		ADMIN				
U	Mai	MITARBEITER		11.10.2007	31.12.9999	
U	Da	MITARBEITER		02.05.2011	30.12.2099	
U	Na	MITARBEITER		01.01.2012	30.12.2050	

=> CHECK in den Stammsätzen: **S_TCODE**

Transaktionscodes fehlen bei allen, außer bei HS11xx (Einkäufer-KeyUser mit Recht auf RE-Buchung und Zahllauf) und den letzten beiden Personen (Moduladministrations-Fkt.)

Substitution von F-Transaktionen selten, möglich hauptsächlich bei M-Transaktionen per SA38, OODR…

IMMER alle Treffer in den Stammsätzen in SUIM überprüfen, indem alle Objekte mit Ausprägungen und Einzelrollen-herkunft herausgelöst werden + TCODEs + Substitutionen suchen, ob aufrufbar !

Bilder beim Vorgehen

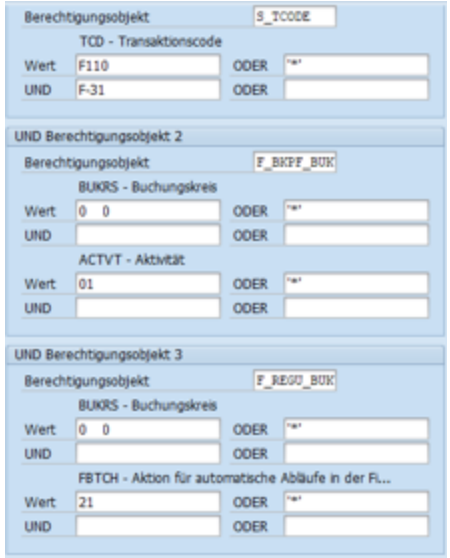
Teilstränge sind auch kritisch!

Reduzierung auf Nur RE + ZL:

Benutzer	Vollständiger Name	Ben. Gruppe	Gesperrt	Gültig von	Gültig bis	Abteilung
H	Nicc	MITARBEITER		30.12.1899	31.12.9999	
H		ADMIN			31.12.9999	
H	Jan	MITARBEITER		30.12.1899	31.12.9999	
HS11	Cars	MITARBEITER		15.10.2007	31.12.9999	EK
	Siby	MITARBEITER		30.12.1899	31.12.9999	
	Ro	MITARBEITER		16.05.2003	31.12.9999	
		NOTFALL				
		ADMIN				
	Nic	MITARBEITER		24.11.2020	30.12.2999	
U	Joh	MITARBEITER		13.01.2021	31.12.9999	V
	Pa	MITARBEITER		21.12.2021	31.12.9999	
	El	MITARBEITER		01.01.2022	31.12.9999	
	To	MITARBEITER		21.12.2021	31.12.9999	
U	Ber	MITARBEITER		19.04.2022	31.12.9999	V
	Birt	MITARBEITER		01.09.2022	31.12.9999	
	Pau	MITARBEITER		01.10.2022	30.09.2023	
	Lu	MITARBEITER		01.01.2023	31.12.9999	
	Ju	MITARBEITER		15.04.2023	31.12.9999	
		ADMIN				
U	Sopl	MITARBEITER		30.12.1899	31.12.9999	

(Auszug)

Bsp.:



EK-Mitarbeiter + 2x aus V-xx = Vertriebsbereich:
V soll nur für 1 Tochter RE und Zahllauf bearbeiten, darf jedoch dies <u>für alle</u> Gesellschaften durchführen
(Rest der Personen aus Finanzbereich/Buchhaltung/Steuern)

Analyse: Zu viele Einzelrollen im Arbeitsplatz, daher **Notwendigkeit des Neuaufbau**s der Arbeitsplatz-rolle für V, sonst dauerhaft Risiko zu hoch!

Muss **Steuerbereich** buchen + ZL können? Eingrenzung für Buchung nicht praktikabel, daher schwierig! ZL nein.
(+ weitere Stränge ausprobieren)

➔ z.B. zusätzlich ggf. M_BEST_BSA mit 01 oder '*' und NNNN oder '*' + TCODE ME21N

Handlungsoption Rollen – Was kann ich bei Treffern tun?

1. Nicht plausibel zugewiesene Arbeitsplatzrolle entfernen

2. Wie Folie zuvor ein Neuaufbau einer Arbeitsplatzrolle

Dies ist notwendig, wenn die stark ausgeprägten Objekte in der Rolle aus einer Vielzahl von Einzelrollen gespeist werden und viele / alle Einzelrollen (in etwa) identisch-hohe Rechte bereitstellen und sich mit den anderen zusammenbauen!

3. Einzelrolle aus Arbeitsplatzrolle entfernen

Wird das ausschlaggebende Berechtigungsobjekt nur aus einer Einzelrolle gespeist, kann es aus der Arbeitsplatzrolle entfernt werden. Ist es aber eine Arbeitsplatzrolle, die für mehrere Arbeiten im Bereich genutzt wird und wenige Leute benötigen das Recht, geht das Entziehen nicht. Ggf. Objekttrennung in separate Einzelrollen.

4. Aus Einzelrolle Objektausprägung entfernen

Dies ist dann möglich, wenn die Einzelrolle, die angepasst wird, nicht woanders genutzt wird, sodass dort das fehlende Objekt zu Funktionsengpässen führt, oder wenn die Objektausprägung in der Arbeitsplatzrolle, die das Recht benötigt, aus einer anderen Einzelrolle zusätzlich gespeist wird und der Entzug keine negative Folge hat.

Hinweis

Sofern eine Person zwei bzw. mehrere manipulierende Rollen aufweist, die nicht zusammen in einer Hand liegen sollten, so ist es keine Lösung, die Rollen auf mehrere UserIDs derselben Person zuzuweisen. Es ist keine Lösung, wenn für dieselbe Person zwei UserIDs eingerichtet werden, die jeweils eine der kritischen Rollen aufnehmen. In den Hitlisten ist die UserID das Gruppierungsmerkmal. In einem solchen Fall würde die Person nicht mehr als SoD-kritisch auftauchen, weil sie ja zwei oder mehrere UserIDs aufweist, die jeweils nur eine kritische Rolle beinhaltet. Trotzdem ist es dieselbe Person, die – nun im UserID-Wechsel – die Funktionalität nacheinander aufrufen kann. Es handelt sich also dann um eine Verschleierung, aber nicht um eine Lösung dieses Funktionalaufrufkonfliktes. Es ist wichtig zu erkennen, dass dies keine Lösung des Problems ist.

VORGEHEN IN DER TRIGGERROLLEN-ANALYSE

Tabellen wie USOBT, TSTC, TDDAT, TRDIR [...] wichtig!

Bestellanforderung	→ Lieferant	→ Bestellung (Rahmenvertrag)	→ Wareneingang	→ Rechnung	→ Zahllauf
M_BANF*	F_LFA1*	M_BEST* (, M_RAHM*)	M_MSEG*	F_BKPF*	F_REGU*

[*Auch zusammenhängende Teile des Prozesses sind ggf. als kritikal zu sehen*]

Suche nach: Aktivität / ACTVT: 01 (hinzufügen), "*" (Generalberechtigung), BUKRS- und KOART-Begrenzungen beachten
02 wird in Vielzahl von **Fachbereichseinzelrollen** vorhanden sein, daher nicht zur **Identifikation** der „First Class"-**Triggerrollen** maßgeblich! Die Einzelrollenausprägungen selbst sind verständlich.

Tabellen AGR_AGRS (Einzelrollen als Child), AGR_DEFINE, AGR_USERS und USER_ADDR zur Feststellung neuralgischer **Arbeitsplatzrollen**

S_TCODE einbeziehen: M*, F* = wichtig: Identifikation der verwendeten, kritischen Transaktionen, aber auch SE16, OODR etc. beachten

Ergebnis: Userstamm-Schnittmengen = Die wenigen User, bei denen der **Verdacht des SoD-Konflikts** erkennbar ist.
Finales Überprüfen im Stammsatz, ob alle für den Funktionsaufruf notwendigen Ausprägungen vorhanden sind !

Fragen ?

Herzlichen Dank für Ihre Aufmerksamkeit.

Rückfragen gern per Mail.

Anlage – Objekte zur Analyse

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 "*"
	Einkaufsorganisation	"*" 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 "*"
	Berechtigungsgruppe	"*" oder Einträge gem. Tabelle TBRG
F_BKPF_BEK	Aktivität	01 (Anlegen), 77 (Vorerfassen) oder "*"
	Berechtigungsgruppe	"*" oder Einträge gem. Tabelle TBRG
F_BKPF_BLA	Aktivität	01 (Anlegen), 10 (Buchen), 43 (Freigeben) oder "*"
	Berechtigungsgruppe	"*" 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

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

Mögliche Ausprägungen FBTCH