MARC GITTLER

IT Prüfungshandlungen für „Nicht IT'ler"

Wie können (einfache) IT Prüfungshandlungen von Nicht-IT-Prüfern durchgeführt werden?

Dipl. Kfm. (FH) Marc Gittler, *CIA, CFSA, CRMA, ist Senior Expert in der Konzernrevision der Deutschen Post DHL Group. Dort ist er verantwortlich für die Themen Finanzen, IT und Filialen im Bereich Post-eCommerce – Parcel. Er ist außerdem Mitglied und stellv. Arbeitskreisleiter des DIIR Arbeitskreises „Continuous Monitoring".*

Gerade in kleineren Revisionseinheiten lassen es Personal- oder Zeitbudgets nicht zu, dass ein Mitarbeiter für reine IT Prüfungen eingestellt werden kann. Doch gerade in der heutigen Zeit, wo die meisten Prozesse nur mit IT-Unterstützung funktionieren, wäre es grob fahrlässig, den IT-Teil einer Prüfung zu vernachlässigen. Der folgende Beitrag soll zeigen, wie einfache Prüfungshandlungen in Prozessprüfungen eingebunden werden können. Dies soll im Folgenden anhand der Bereiche System-Berechtigungen und Individuelle Datenverarbeitung (IDV) verdeutlicht werden. Für beide Bereiche werden nach einer allgemeinen Einführung Prüfungshandlungen für SAP Systeme und Excel Dateien dargestellt. Weiterhin werden weitere Prüfungshandlungen aus den Bereichen Datensicherung und Datensicherheit aufgezeigt.

1. Grundlagen

In der heutigen Zeit sind Prozesse, die nicht in irgendeiner Art und Weise von IT Systemen unterstützt werden, kaum vorstellbar. Selbst wenn der Primärprozess nicht IT-unterstützt funktioniert, so ist die Wahrscheinlichkeit, dass die Sekundärprozesse IT enthalten – und sei es nur eine vom Mitarbeiter selbst erstellte Excel Datei – sehr hoch.

Die Notwendigkeit auch IT-Prüfungshandlungen durchzuführen ergibt sich aus einer Vielzahl von gesetzlichen und regulatorischen Vorgaben. Exemplarisch seinen hier der § 91 Abs. 2 AktG genannt, nach dem der Vorstand geeignete Maßnahmen, insbesondere ein internes Überwachungssystem, einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

2. Prüfen von Berechtigungen

Sinn und Zweck eines jeden Berechtigungskonzeptes ist es, einem Benutzer nur Rechte auf ein System zuzuweisen, die er tatsächlich für seine Arbeit benötigt. Dabei kann die Art der Autorisierung noch weiter spezifiziert werden (beispielsweise Lese- oder Schreibrechte auf bestimmte Bereiche). Natürlich ist es in den meisten Fällen Revisionsabteilungen, die keine Spezialisten für derartige Prüfungen besitzen, nicht möglich, ein existierendes Berechtigungskonzept vollumfänglich zu prüfen. Dennoch gibt es Fragestellungen, die auch von nicht spezialisierten Prüfern im Rahmen von z. B. Prozessprüfungen abgearbeitet werden können:

- Gibt es eine dokumentierte Berechtigungsstruktur, die regelt, welche Benutzer auf welche Daten zugreifen können?
- Erfolgt die Änderung von Benutzerberechtigungen schriftlich?
- Werden die Berechtigungen regelmäßig unabhängig überprüft?
- Ist ein Prozess für Rechtevergabe und besonders für den Entzug der Rechte (Ausscheiden aus dem Unternehmen, Versetzung) vorhanden?

Gerade auf den in Punkt 4 genannten Sachverhalt des Entzuges von Berechtigungen sollte ein besonderes Augenmerk gelegt werden, da dies meist der Teilprozessschritt ist, dem am wenigsten Aufmerksamkeit geschenkt wird. Besonders fatale Auswirkungen hat dies im Falle von Versetzungen, da dann die Gefahr besteht, dass die alten Rechte in Verbindung mit den Rechten für die neue Tätigkeit in Konflikt stehen und so die eigentlich vorgesehenen Kontrollen des Internen-Kontroll-Systems aushebeln.

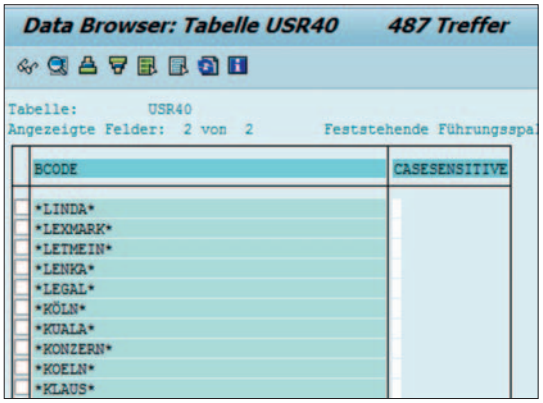


Abbildung 1: *Inhalt der Tabelle USR 40*

Im Folgenden sollen exemplarische Prüfungshandlungen für SAP Systeme gezeigt werden, die sich auf den Bereich „Berechtigungen" beziehen. Diese sollten auch für nicht IT-Prüfer durchführbar sein und decken zumindest einen Teil der möglichen Risiken ab.

Kritische Passwörter

Normalerweise sollten Richtlinien für die Vergabe von Passwörtern existieren. Ziel einer solche Richtlinie ist i.d.R. die Sicherstellung eines notwendigen Sicherheitsniveaus für den Einsatz von Benutzername und/oder Passwort. Dies kann beispielsweise durch die Vorgabe von Mindestlängen oder der Vorgabe zur Benutzung von besonderen Zeichen (groß, klein, Sonderzeichen) erfolgen. Allerdings sollten bereits systemseitig bestimmte Wörter gesperrt werden (z. B. „Monate", „Admin", „Administrator", 12345, etc.). Genau diese Möglichkeit bietet SAP in der Tabelle USR 40. Je besser eine solche „Blacklist" gepflegt ist, desto schwieriger wird es beispielsweise Kennwörter anderer Mitarbeiter zu erraten, um so Kontrollen zu umgehen. Im Rahmen einer Prüfung sollte sich ein Prüfer also ansehen, wie genau diese Liste gepflegt ist. Dies kann er zum Beispiel in dem er die Tabelle USR 40 mittels der Transaktion SE 16 aufruft und den Inhalt der Tabelle bewertet (vgl. Abbildung 1).

Kritische Berechtigungen

Wie bereits oben geschrieben, dient ein Berechtigungskonzept im Kern dazu, Benutzer nur die Informationen zur Verfügung zu stellen, die tatsächlich für die entsprechenden Tätigkeiten benötigt werden. Dies wird in der Regel über die Vergabe von Rollen (oder Profilen) erreicht. Da eine Prüfung des Rollenkonzeptes sicherlich eine hoch komplexe Tätigkeit darstellt, die nur von entsprechenden Spezialisten durchgeführt werden sollte,

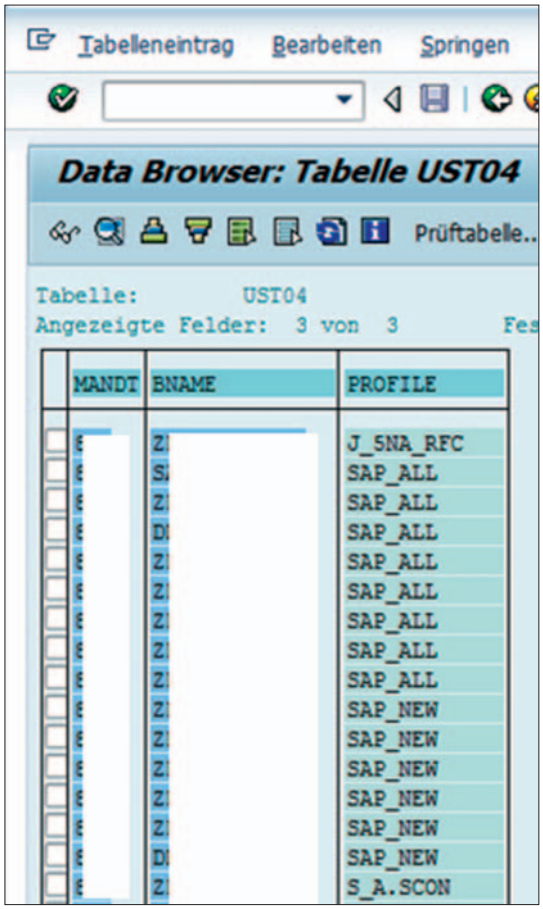
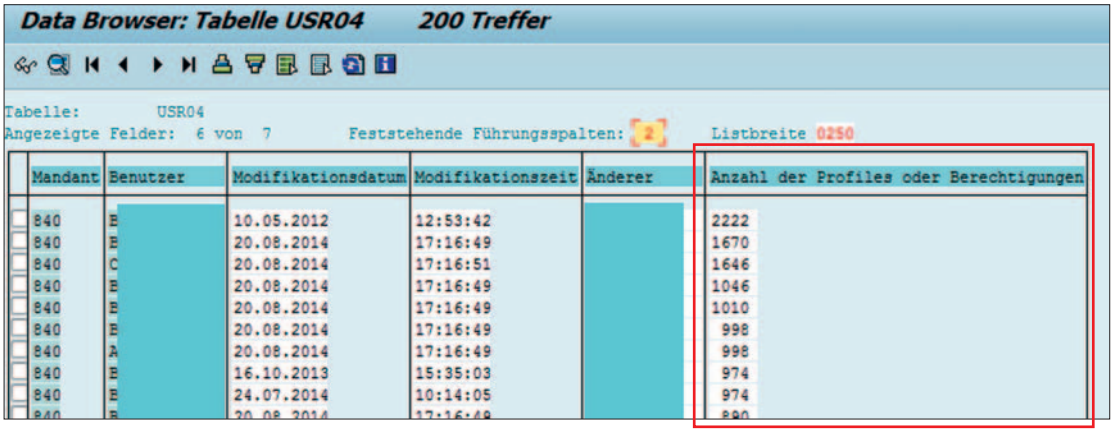


Abbildung 2: *SAP Tabelle UST 04*

wird hier dargestellt, wie man anhand der vergebenen Rollen, diejenigen identifizieren kann, die es dem entsprechenden Nutzer erlauben, evtl. nicht vorgesehene Tätigkeiten im System auszuüben. Auch hier kann der Prüfer durch die Transaktion SE 16 die entsprechende Tabelle UST 04 im SAP Data Browser aufrufen (vgl. Abbildung 2).

Anschließend (ggf. nach einem Export nach Excel) kann der Prüfer nach kritischen Profilen suchen. Kritische Profile könnten z. B. sein:

- SAP* (SAP Super User): SAP* ist der einzige Benutzer im SAP-System, für den kein Benutzerstammsatz erforderlich ist, da er im Systemcode definiert ist. SAP* hat standardmäßig das Kennwort PASS sowie uneingeschränkte Zugriffsberechtigungen auf das System.
- SAP_ALL: enthält alle SAP-Berechtigungen, so dass ein Benutzer mit diesem Profil im SAP-System alle Aufgaben durchführen kann.
- SAP_NEW: Dieses Sammelprofil enthält je Release ein Einzelprofil, das diejenigen Berechtigungen enthält, die die Benutzer benötigen, um die bisherigen Funktionen, die mit neuen Berechtigungsprüfungen geschützt sind, weiter verwenden zu können.



Data Browser: Tabelle USR04 200 Treffer

Tabelle: USR04
Angezeigte Felder: 6 von 7 Feststehende Führungsspalten: 2 Listbreite 0250

Mandant	Benutzer	Modifikationsdatum	Modifikationszeit	Änderer	Anzahl der Profiles oder Berechtigungen
840	B	10.05.2012	12:53:42		2222
840	B	20.08.2014	17:16:49		1670
840	C	20.08.2014	17:16:51		1646
840	B	20.08.2014	17:16:49		1046
840	B	20.08.2014	17:16:49		1010
840	B	20.08.2014	17:16:49		998
840	A	20.08.2014	17:16:49		998
840	B	16.10.2013	15:35:03		974
840	B	24.07.2014	10:14:05		974
840	B	20.08.2014	17:16:49		890

Abbildung 3: *SAP Tabelle USR 04*

- S_DEVELOP: Allgemeines Berechtigungsobjekt für Objekte der ABAP Development Workbench. Mit diesem Objekt können Sie Zugriffsberechtigungen für alle Komponenten der Workbench erteilen.
- S_PROGRAM: Berechtigung, ABAP/4-Programme nach Programmgruppen auszuführen

Da die Tabelle UST 04 neben den Profilen auch den entsprechenden Namen bzw. dessen SAP Usernamen enthält ist es mit relativ einfachen Mitteln (z. B. Abgleich mit Telefonbuch des Unternehmens) möglich zu prüfen, ob der entsprechende Mitarbeiter diese Berechtigung tatsächlich benötigt. So ist es sicherlich in Ordnung, wenn eine begrenzte Zahl von Mitarbeitern in der IT-Abteilung über das Profil SAP_ALL verfügt, da er es beispielsweise für seine Tätigkeiten als SAP Administrator diese Rechte benötigt.

Kritische Nutzer

Eine weitere Möglichkeit Nutzer zu identifizieren, die ggf. zu viele Berechtigungen im System haben ist es sich in der Tabelle USR 04 die Anzahl der Profile oder Berechtigungen anzeigen zu lassen. Sollten dabei einige Nutzer durch eine hohe Zahl von Berechtigungen im Vergleich zu den anderen Nutzern auffallen (vgl. Abbildung 3), sollten diese ebenfalls einer besonderen Prüfung unterzogen werden.

Einen weiteren Hinweis auf Benutzer, die ggf. nicht mehr den Zugang zu einem bestimmten System benötigen gibt die Tabelle USR 02 (vgl. Abbildung 4). In dieser Tabelle wird angezeigt, wann sich der entsprechende Nutzer das letze Mal in dem System angemeldet hat.

Die Auswertung dieser Tabelle kann einen Aufschluss über das Funktionieren des bereits erwähnten Entzuges von Berechtigungen sein. Nutzer, die sich längere Zeit nicht mehr angemeldet haben, können darauf untersucht werden, ob sie beispielsweise noch im Unternehmen beschäftigt sind. Wird festgestellt, dass ein Ausscheiden aus dem Unternehmen ein häufiger Grund für lange Phasen der Nichtnutzung ist, sollte der Prozess zum Entzug von Berechtigungen genauer untersucht werden.

Kritische Transaktionskombinationen

Ein SAP System bietet die Möglichkeit an, automatisiert nach Benutzern zu suchen, die die Berechtigungen besitzen, bestimmte Kombinationen von Transaktionen aufzurufen. Dazu ist über die Transaktion SU 98 (Pflege der Tabelle SUKRI) eine Liste der kritischen Kombinationen zu pflegen. Über den Report „RSUSR 008_009_new" lassen sich dann die Benutzer identifizieren, die die kritischen SAP Berechtigungskombinationen besitzen.

3. Weitere Prüffelder ausserhalb von SAP

Neben den aufgezeigten Prüfschritten bei Berechtigungsprüfungen bieten sich auch andere Themen an, in eine „non IT"-Prüfung einbezogen zu werden.

Netzlaufwerke

Oft werden Daten nicht auf dem eigenen PC oder Laptop vorgehalten, sondern auf Netzlaufwerken z. B. der ganzen Abteilung zugänglich gemacht. Sollten also Daten auf solchen Laufwerken während einer Prüfung festgestellt werden, so sollten sich auch nicht IT-Prüfer folgende Fragen stellen und die Antworten entsprechend bewerten:

- Welche Daten werden vorgehalten (Kritikalität)?
- Wer hat Zugriff?